

EXHIBIT A

SUMMONS
(CITACION JUDICIAL)

NOTICE TO DEFENDANT:
(AVISO AL DEMANDADO):

SAMSUNG ELECTRONICS AMERICA, INC., a New York corporation; and
DOES 1 through 100, inclusive;

YOU ARE BEING SUED BY PLAINTIFF:
(LO ESTÁ DEMANDANDO EL DEMANDANTE):

RAFFI KELECHIAN, individually, and on behalf of all others similarly situated;

NOTICE! You have been sued. The court may decide against you without your being heard unless you respond within 30 days. Read the information below.

You have 30 CALENDAR DAYS after this summons and legal papers are served on you to file a written response at this court and have a copy served on the plaintiff. A letter or phone call will not protect you. Your written response must be in proper legal form if you want the court to hear your case. There may be a court form that you can use for your response. You can find these court forms and more information at the California Courts Online Self-Help Center (www.courtinfo.ca.gov/selfhelp), your county law library, or the courthouse nearest you. If you cannot pay the filing fee, ask the court clerk for a fee waiver form. If you do not file your response on time, you may lose the case by default, and your wages, money, and property may be taken without further warning from the court.

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site (www.lawhelpcalifornia.org), the California Courts Online Self-Help Center (www.courtinfo.ca.gov/selfhelp), or by contacting your local court or county bar association. **NOTE:** The court has a statutory lien for waived fees and costs on any settlement or arbitration award of \$10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case.

¡AVISO! Lo han demandado. Si no responde dentro de 30 días, la corte puede decidir en su contra sin escuchar su versión. Lea la información a continuación.

Tiene 30 DÍAS DE CALENDARIO después de que le entreguen esta citación y papeles legales para presentar una respuesta por escrito en esta corte y hacer que se entregue una copia al demandante. Una carta o una llamada telefónica no lo protegen. Su respuesta por escrito tiene que estar en formato legal correcto si desea que procesen su caso en la corte. Es posible que haya un formulario que usted pueda usar para su respuesta. Puede encontrar estos formularios de la corte y más información en el Centro de Ayuda de las Cortes de California (www.sucorte.ca.gov), en la biblioteca de leyes de su condado o en la corte que le quede más cerca. Si no puede pagar la cuota de presentación, pida al secretario de la corte que le dé un formulario de exención de pago de cuotas. Si no presenta su respuesta a tiempo, puede perder el caso por incumplimiento y la corte le podrá quitar su sueldo, dinero y bienes sin más advertencia.

Hay otros requisitos legales. Es recomendable que llame a un abogado inmediatamente. Si no conoce a un abogado, puede llamar a un servicio de remisión a abogados. Si no puede pagar a un abogado, es posible que cumpla con los requisitos para obtener servicios legales gratuitos de un programa de servicios legales sin fines de lucro. Puede encontrar estos grupos sin fines de lucro en el sitio web de California Legal Services (www.lawhelpcalifornia.org), en el Centro de Ayuda de las Cortes de California (www.sucorte.ca.gov) o poniéndose en contacto con la corte o el colegio de abogados locales. **AVISO:** Por ley, la corte tiene derecho a reclamar las cuotas y los costos exentos por imponer un gravamen sobre cualquier recuperación de \$10,000 ó más de valor recibida mediante un acuerdo o una concesión de arbitraje en un caso de derecho civil. Tiene que pagar el gravamen de la corte antes de que la corte pueda desechar el caso.

The name and address of the court is:
(El nombre y dirección de la corte es):

CASE NUMBER
(Número del Caso):

22STCV30284

Stanley Mosk Courthouse, 111 N. Hill St., Los Angeles, CA 90012

The name, address, and telephone number of plaintiff's attorney, or plaintiff without an attorney, is:

(El nombre, la dirección y el número de teléfono del abogado del demandante, o del demandante que no tiene abogado, es):
Daniel Srourian, Srourian Law Firm, 3435 Wilshire Blvd. Suite 1710, Los Angeles, CA 90010. (213) 474-3800

Sherri R. Carter Executive Officer / Clerk of Court

DATE: 09/16/2022
(Fecha)

Clerk, by R. Lozano, Deputy
(Secretario) (Adjunto)

(For proof of service of this summons, use Proof of Service of Summons (form POS-010).)

(Para prueba de entrega de esta citación use el formulario Proof of Service of Summons, (POS-010)).

[SEAL]



NOTICE TO THE PERSON SERVED: You are served

1. ☐ as an individual defendant.
2. ☐ as the person sued under the fictitious name of (specify):

3. ☐ on behalf of (specify):

under: ☐ CCP 416.10 (corporation) ☐ CCP 416.60 (minor)
☐ CCP 416.20 (defunct corporation) ☐ CCP 416.70 (conservatee)
☐ CCP 416.40 (association or partnership) ☐ CCP 416.90 (authorized person)
☐ other (specify):

4. ☐ by personal delivery on (date):

VOLUNTARY EFFICIENT LITIGATION STIPULATIONS



Superior Court of California
County of Los Angeles

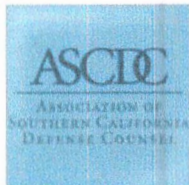


Los Angeles County
Bar Association
Litigation Section

Los Angeles County
Bar Association Labor and
Employment Law Section



Consumer Attorneys
Association of Los Angeles



Southern California
Defense Counsel



Association of
Business Trial Lawyers



California Employment
Lawyers Association

The Early Organizational Meeting Stipulation, Discovery Resolution Stipulation, and Motions in Limine Stipulation are voluntary stipulations entered into by the parties. The parties may enter into one, two, or all three of the stipulations; however, they may not alter the stipulations as written, because the Court wants to ensure uniformity of application. These stipulations are meant to encourage cooperation between the parties and to assist in resolving issues in a manner that promotes economic case resolution and judicial efficiency.

The following organizations endorse the goal of promoting efficiency in litigation and ask that counsel consider using these stipulations as a voluntary way to promote communications and procedures among counsel and with the court to fairly resolve issues in their cases.

◆ Los Angeles County Bar Association Litigation Section ◆

◆ Los Angeles County Bar Association
Labor and Employment Law Section ◆

◆ Consumer Attorneys Association of Los Angeles ◆

◆ Southern California Defense Counsel ◆

◆ Association of Business Trial Lawyers ◆

◆ California Employment Lawyers Association ◆

NAME AND ADDRESS OF ATTORNEY OR PARTY WITHOUT ATTORNEY:		STATE BAR NUMBER	Reserved for Clerk's File Stamp
TELEPHONE NO. E-MAIL ADDRESS (Optional) ATTORNEY FOR (Name):		FAX NO. (Optional):	
SUPERIOR COURT OF CALIFORNIA, COUNTY OF LOS ANGELES			
COURTHOUSE ADDRESS:			
PLAINTIFF:			
DEFENDANT:			CASE NUMBER:
STIPULATION – EARLY ORGANIZATIONAL MEETING			

This stipulation is intended to encourage cooperation among the parties at an early stage in the litigation and to assist the parties in efficient case resolution.

The parties agree that:

1. The parties commit to conduct an initial conference (in-person or via teleconference or via videoconference) within 15 days from the date this stipulation is signed, *to discuss and consider whether there can be agreement on the following:*
 - a. Are motions to challenge the pleadings necessary? If the issue can be resolved by amendment as of right, or if the Court would allow leave to amend, could an amended complaint resolve most or all of the issues a demurrer might otherwise raise? If so, the parties agree to work through pleading issues so that a demurrer need only raise issues they cannot resolve. Is the issue that the defendant seeks to raise amenable to resolution on demurrer, or would some other type of motion be preferable? Could a voluntary targeted exchange of documents or information by any party cure an uncertainty in the pleadings?
 - b. Initial mutual exchanges of documents at the "core" of the litigation. (For example, in an employment case, the employment records, personnel file and documents relating to the conduct in question could be considered "core." In a personal injury case, an incident or police report, medical records, and repair or maintenance records could be considered "core.");
 - c. Exchange of names and contact information of witnesses;
 - d. Any insurance agreement that may be available to satisfy part or all of a judgment, or to indemnify or reimburse for payments made to satisfy a judgment;
 - e. Exchange of any other information that might be helpful to facilitate understanding, handling, or resolution of the case in a manner that preserves objections or privileges by agreement;
 - f. Controlling issues of law that, if resolved early, will promote efficiency and economy in other phases of the case. Also, when and how such issues can be presented to the Court;
 - g. Whether or when the case should be scheduled with a settlement officer, what discovery or court ruling on legal issues is reasonably required to make settlement discussions meaningful, and whether the parties wish to use a sitting judge or a private mediator or other options as

SHORT TITLE	CASE NUMBER
-------------	-------------

discussed in the "Alternative Dispute Resolution (ADR) Information Package" served with the complaint;

- h. Computation of damages, including documents, not privileged or protected from disclosure, on which such computation is based;
 - i. Whether the case is suitable for the Expedited Jury Trial procedures (see information at www.lacourt.org under "Civil" and then under "General Information").
2. The time for a defending party to respond to a complaint or cross-complaint will be extended to _____ for the complaint, and _____ for the cross-complaint, which is comprised of the 30 days to respond under Government Code § 68616(b), and the 30 days permitted by Code of Civil Procedure section 1054(a), good cause having been found by the Civil Supervising Judge due to the case management benefits provided by this Stipulation. A copy of the General Order can be found at www.lacourt.org under "Civil", click on "General Information", then click on "Voluntary Efficient Litigation Stipulations".
 3. The parties will prepare a joint report titled "Joint Status Report Pursuant to Initial Conference and Early Organizational Meeting Stipulation, and if desired, a proposed order summarizing results of their meet and confer and advising the Court of any way it may assist the parties' efficient conduct or resolution of the case. The parties shall attach the Joint Status Report to the Case Management Conference statement, and file the documents when the CMC statement is due.
 4. References to "days" mean calendar days, unless otherwise noted. If the date for performing any act pursuant to this stipulation falls on a Saturday, Sunday or Court holiday, then the time for performing that act shall be extended to the next Court day

The following parties stipulate:

Date:

_____	➤	_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR PLAINTIFF)
Date: _____	➤	_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR DEFENDANT)
Date: _____	➤	_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR DEFENDANT)
Date: _____	➤	_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR DEFENDANT)
Date: _____	➤	_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR _____)
Date: _____	➤	_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR _____)
Date: _____	➤	_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR _____)

NAME AND ADDRESS OF ATTORNEY OR PARTY WITHOUT ATTORNEY:		STATE BAR NUMBER	Reserved for Clerk's File Stamp
TELEPHONE NO.:		FAX NO. (Optional):	
E-MAIL ADDRESS (Optional):			
ATTORNEY FOR (Name):			
SUPERIOR COURT OF CALIFORNIA, COUNTY OF LOS ANGELES			
COURTHOUSE ADDRESS:			
PLAINTIFF:			
DEFENDANT:			
STIPULATION – DISCOVERY RESOLUTION			CASE NUMBER:

This stipulation is intended to provide a fast and informal resolution of discovery issues through limited paperwork and an informal conference with the Court to aid in the resolution of the issues.

The parties agree that:

1. Prior to the discovery cut-off in this action, no discovery motion shall be filed or heard unless the moving party first makes a written request for an Informal Discovery Conference pursuant to the terms of this stipulation.
2. At the Informal Discovery Conference the Court will consider the dispute presented by parties and determine whether it can be resolved informally. Nothing set forth herein will preclude a party from making a record at the conclusion of an Informal Discovery Conference, either orally or in writing.
3. Following a reasonable and good faith attempt at an informal resolution of each issue to be presented, a party may request an Informal Discovery Conference pursuant to the following procedures:
 - a. The party requesting the Informal Discovery Conference will:
 - i. File a Request for Informal Discovery Conference with the clerk's office on the approved form (copy attached) and deliver a courtesy, conformed copy to the assigned department;
 - ii. Include a brief summary of the dispute and specify the relief requested; and
 - iii. Serve the opposing party pursuant to any authorized or agreed method of service that ensures that the opposing party receives the Request for Informal Discovery Conference no later than the next court day following the filing.
 - b. Any Answer to a Request for Informal Discovery Conference must:
 - i. Also be filed on the approved form (copy attached);
 - ii. Include a brief summary of why the requested relief should be denied;

SHORT TITLE	CASE NUMBER
-------------	-------------

- iii. Be filed within two (2) court days of receipt of the Request; and
 - iv. Be served on the opposing party pursuant to any authorized or agreed upon method of service that ensures that the opposing party receives the Answer no later than the next court day following the filing.
- c. No other pleadings, including but not limited to exhibits, declarations, or attachments, will be accepted.
- d. If the Court has not granted or denied the Request for Informal Discovery Conference within ten (10) days following the filing of the Request, then it shall be deemed to have been denied. If the Court acts on the Request, the parties will be notified whether the Request for Informal Discovery Conference has been granted or denied and, if granted, the date and time of the Informal Discovery Conference, which must be within twenty (20) days of the filing of the Request for Informal Discovery Conference.
- e. If the conference is not held within twenty (20) days of the filing of the Request for Informal Discovery Conference, unless extended by agreement of the parties and the Court, then the Request for the Informal Discovery Conference shall be deemed to have been denied at that time.
4. If (a) the Court has denied a conference or (b) one of the time deadlines above has expired without the Court having acted or (c) the Informal Discovery Conference is concluded without resolving the dispute, then a party may file a discovery motion to address unresolved issues.
5. The parties hereby further agree that the time for making a motion to compel or other discovery motion is tolled from the date of filing of the Request for Informal Discovery Conference until (a) the request is denied or deemed denied or (b) twenty (20) days after the filing of the Request for Informal Discovery Conference, whichever is earlier, unless extended by Order of the Court.
- It is the understanding and intent of the parties that this stipulation shall, for each discovery dispute to which it applies, constitute a writing memorializing a "specific later date to which the propounding [or demanding or requesting] party and the responding party have agreed in writing," within the meaning of Code Civil Procedure sections 2030.300(c), 2031.320(c), and 2033.290(c).
6. Nothing herein will preclude any party from applying *ex parte* for appropriate relief, including an order shortening time for a motion to be heard concerning discovery.
7. Any party may terminate this stipulation by giving twenty-one (21) days notice of intent to terminate the stipulation.
8. References to "days" mean calendar days, unless otherwise noted. If the date for performing any act pursuant to this stipulation falls on a Saturday, Sunday or Court holiday, then the time for performing that act shall be extended to the next Court day.

SHORT TITLE:	CASE NUMBER:
--------------	--------------

The following parties stipulate:

Date:	➤	
_____		_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR PLAINTIFF)
Date:	➤	
_____		_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR DEFENDANT)
Date:	➤	
_____		_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR DEFENDANT)
Date:	➤	
_____		_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR DEFENDANT)
Date:	➤	
_____		_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR _____)
Date:	➤	
_____		_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR _____)
Date:	➤	
_____		_____
(TYPE OR PRINT NAME)		(ATTORNEY FOR _____)

Print **Save**

Clear

NAME AND ADDRESS OF ATTORNEY OR PARTY WITHOUT ATTORNEY:		STATE BAR NUMBER	Reserved for Clerk's File Stamp
TELEPHONE NO. : E-MAIL ADDRESS (Optional): ATTORNEY FOR (Name):		FAX NO. (Optional):	
SUPERIOR COURT OF CALIFORNIA, COUNTY OF LOS ANGELES			
COURTHOUSE ADDRESS:			
PLAINTIFF:			
DEFENDANT:			CASE NUMBER:
INFORMAL DISCOVERY CONFERENCE (pursuant to the Discovery Resolution Stipulation of the parties)			

1. This document relates to:

☐
☐

Request for Informal Discovery Conference
 Answer to Request for Informal Discovery Conference

2. Deadline for Court to decide on Request: _____ (insert date 10 calendar days following filing of the Request).
3. Deadline for Court to hold Informal Discovery Conference: _____ (insert date 20 calendar days following filing of the Request).
4. For a Request for Informal Discovery Conference, briefly describe the nature of the discovery dispute, including the facts and legal arguments at issue. For an Answer to Request for Informal Discovery Conference, briefly describe why the Court should deny the requested discovery, including the facts and legal arguments at issue.

NAME AND ADDRESS OF ATTORNEY OR PARTY WITHOUT ATTORNEY:		STATE BAR NUMBER	Reserved for Clerk's File Stamp
TELEPHONE NO. : E-MAIL ADDRESS (Optional): ATTORNEY FOR (Name):		FAX NO. (Optional):	
SUPERIOR COURT OF CALIFORNIA, COUNTY OF LOS ANGELES			
COURTHOUSE ADDRESS:			
PLAINTIFF:			
DEFENDANT:			CASE NUMBER:
STIPULATION AND ORDER – MOTIONS IN LIMINE			

This stipulation is intended to provide fast and informal resolution of evidentiary issues through diligent efforts to define and discuss such issues and limit paperwork.

The parties agree that:

1. At least ____ days before the final status conference, each party will provide all other parties with a list containing a one paragraph explanation of each proposed motion in limine. Each one paragraph explanation must identify the substance of a single proposed motion in limine and the grounds for the proposed motion.
2. The parties thereafter will meet and confer, either in person or via teleconference or videoconference, concerning all proposed motions in limine. In that meet and confer, the parties will determine:
 - a. Whether the parties can stipulate to any of the proposed motions. If the parties so stipulate, they may file a stipulation and proposed order with the Court.
 - b. Whether any of the proposed motions can be briefed and submitted by means of a short joint statement of issues. For each motion which can be addressed by a short joint statement of issues, a short joint statement of issues must be filed with the Court 10 days prior to the final status conference. Each side's portion of the short joint statement of issues may not exceed three pages. The parties will meet and confer to agree on a date and manner for exchanging the parties' respective portions of the short joint statement of issues and the process for filing the short joint statement of issues.
3. All proposed motions in limine that are not either the subject of a stipulation or briefed via a short joint statement of issues will be briefed and filed in accordance with the California Rules of Court and the Los Angeles Superior Court Rules.

SHORT TITLE	CASE NUMBER
-------------	-------------

The following parties stipulate:

Date:

(TYPE OR PRINT NAME)

Date:

(TYPE OR PRINT NAME)

Date:

(TYPE OR PRINT NAME)

Date:

(TYPE OR PRINT NAME)

Date:

(TYPE OR PRINT NAME)

Date:

(TYPE OR PRINT NAME)

Date:

(TYPE OR PRINT NAME)

➤

(ATTORNEY FOR PLAINTIFF)

➤

(ATTORNEY FOR DEFENDANT)

➤

(ATTORNEY FOR DEFENDANT)

➤

(ATTORNEY FOR DEFENDANT)

➤

(ATTORNEY FOR _____)

➤

(ATTORNEY FOR _____)

➤

(ATTORNEY FOR _____)

THE COURT SO ORDERS.

Date: _____

JUDICIAL OFFICER

Print

Save

Clear

FILED
LOS ANGELES SUPERIOR COURT

MAY 11 2011

JOHN A. CLARKE, CLERK
N. Navarro
BY NANCY NAVARRO, DEPUTY

**SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES**

General Order Re) ORDER PURSUANT TO CCP 1054(a),
Use of Voluntary Efficient Litigation) EXTENDING TIME TO RESPOND BY
Stipulations) 30 DAYS WHEN PARTIES AGREE
) TO EARLY ORGANIZATIONAL
) MEETING STIPULATION
)

Whereas the Los Angeles Superior Court and the Executive Committee of the Litigation Section of the Los Angeles County Bar Association have cooperated in drafting "Voluntary Efficient Litigation Stipulations" and in proposing the stipulations for use in general jurisdiction civil litigation in Los Angeles County;

Whereas the Los Angeles County Bar Association Litigation Section; the Los Angeles County Bar Association Labor and Employment Law Section; the Consumer Attorneys Association of Los Angeles; the Association of Southern California Defense Counsel; the Association of Business Trial Lawyers of Los Angeles; and the California Employment Lawyers Association all "endorse the goal of promoting efficiency in litigation, and ask that counsel consider using these stipulations as a voluntary way to promote communications and procedures among counsel and with the court to fairly resolve issues in their cases;"

1 Whereas the Early Organizational Meeting Stipulation is intended to encourage
2 cooperation among the parties at an early stage in litigation in order to achieve
3 litigation efficiencies;

4 Whereas it is intended that use of the Early Organizational Meeting Stipulation
5 will promote economic case resolution and judicial efficiency;

6
7 Whereas, in order to promote a meaningful discussion of pleading issues at the
8 Early Organizational Meeting and potentially to reduce the need for motions to
9 challenge the pleadings, it is necessary to allow additional time to conduct the Early
10 Organizational Meeting before the time to respond to a complaint or cross complaint
11 has expired;

12
13 Whereas Code of Civil Procedure section 1054(a) allows a judge of the court in
14 which an action is pending to extend for not more than 30 days the time to respond to
15 a pleading "upon good cause shown";

16 Now, therefore, this Court hereby finds that there is good cause to extend for 30
17 days the time to respond to a complaint or to a cross complaint in any action in which
18 the parties have entered into the Early Organizational Meeting Stipulation. This finding
19 of good cause is based on the anticipated judicial efficiency and benefits of economic
20 case resolution that the Early Organizational Meeting Stipulation is intended to
21 promote.
22

23
24 IT IS HEREBY ORDERED that, in any case in which the parties have entered
25 into an Early Organizational Meeting Stipulation, the time for a defending party to
26 respond to a complaint or cross complaint shall be extended by the 30 days permitted
27
28

1 by Code of Civil Procedure section 1054(a) without further need of a specific court
2 order.

3
4 DATED: May 11, 2011

Carolyn B. Kuhl
Carolyn B. Kuhl, Supervising Judge of the
Civil Departments, Los Angeles Superior Court



Superior Court of California, County of Los Angeles

ALTERNATIVE DISPUTE RESOLUTION (ADR) INFORMATION PACKAGE

THE PLAINTIFF MUST SERVE THIS ADR INFORMATION PACKAGE ON EACH PARTY WITH THE COMPLAINT.

CROSS-COMPLAINANTS must serve this ADR Information Package on any new parties named to the action with the cross-complaint.

What is ADR?

ADR helps people find solutions to their legal disputes without going to trial. The main types of ADR are negotiation, mediation, arbitration, and settlement conferences. When ADR is done by phone, videoconference or computer, it may be called Online Dispute Resolution (ODR). These alternatives to litigation and trial are described below.

Advantages of ADR

- **Saves Time:** ADR is faster than going to trial.
- **Saves Money:** Parties can save on court costs, attorney's fees, and witness fees.
- **Keeps Control** (with the parties): Parties choose their ADR process and provider for voluntary ADR.
- **Reduces Stress/Protects Privacy:** ADR is done outside the courtroom, in private offices, by phone or online.

Disadvantages of ADR

- **Costs:** If the parties do not resolve their dispute, they may have to pay for ADR, litigation, and trial.
- **No Public Trial:** ADR does not provide a public trial or a decision by a judge or jury.

Main Types of ADR

1. **Negotiation:** Parties often talk with each other in person, or by phone or online about resolving their case with a settlement agreement instead of a trial. If the parties have lawyers, they will negotiate for their clients.
2. **Mediation:** In mediation, a neutral mediator listens to each person's concerns, helps them evaluate the strengths and weaknesses of their case, and works with them to try to create a settlement agreement that is acceptable to all. Mediators do not decide the outcome. Parties may go to trial if they decide not to settle.

Mediation may be appropriate when the parties

- want to work out a solution but need help from a neutral person.
- have communication problems or strong emotions that interfere with resolution.

Mediation may not be appropriate when the parties

- want a public trial and want a judge or jury to decide the outcome.
- lack equal bargaining power or have a history of physical/emotional abuse.

How to Arrange Mediation in Los Angeles County

Mediation for **civil cases** is voluntary and parties may select any mediator they wish. Options include:

a. **The Civil Mediation Vendor Resource List**

If all parties in an active civil case agree to mediation, they may contact these organizations to request a "Resource List Mediation" for mediation at reduced cost or no cost (for selected cases).

- **ADR Services, Inc.** Case Manager Elizabeth Sanchez, elizabeth@adrservices.com
(949) 863-9800
- **Mediation Center of Los Angeles** Program Manager info@mediationLA.org
(833) 476-9145

These organizations cannot accept every case and they may decline cases at their discretion. They may offer online mediation by video conference for cases they accept. Before contacting these organizations, review important information and FAQs at www.lacourt.org/ADR.Res.List

NOTE: The Civil Mediation Vendor Resource List program does not accept family law, probate or small claims cases.

b. **Los Angeles County Dispute Resolution Programs**

<https://hrc.lacounty.gov/wp-content/uploads/2020/05/DRP-Fact-Sheet-23October19-Current-as-of-October-2019-1.pdf>

Day of trial mediation programs have been paused until further notice.

Online Dispute Resolution (ODR). Parties in small claims and unlawful detainer (eviction) cases should carefully review the Notice and other information they may receive about (ODR) requirements for their case.

c. Mediators and ADR and Bar organizations that provide mediation may be found on the internet.

3. Arbitration: Arbitration is less formal than trial, but like trial, the parties present evidence and arguments to the person who decides the outcome. In "binding" arbitration, the arbitrator's decision is final; there is no right to trial. In "nonbinding" arbitration, any party can request a trial after the arbitrator's decision. For more information about arbitration, visit <http://www.courts.ca.gov/programs-adr.htm>

4. Mandatory Settlement Conferences (MSC): MSCs are ordered by the Court and are often held close to the trial date or on the day of trial. The parties and their attorneys meet with a judge or settlement officer who does not make a decision but who instead assists the parties in evaluating the strengths and weaknesses of the case and in negotiating a settlement. For information about the Court's MSC programs for civil cases, visit <http://www.lacourt.org/division/civil/C10047.aspx>

Los Angeles Superior Court ADR website: <http://www.lacourt.org/division/civil/C10109.aspx>
For general information and videos about ADR, visit <http://www.courts.ca.gov/programs-adr.htm>

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address): Daniel Srourian, Esq. SBN 285678 SROURIAN LAW FIRM 3435 Wilshire Blvd. Suite 1710 Los Angeles, CA 90010 TELEPHONE NO: 213-474-3800 FAX NO: 213-471-4160 ATTORNEY FOR (Name): Plaintiff Raffi Kelechian			
SUPERIOR COURT OF CALIFORNIA, COUNTY OF Los Angeles STREET ADDRESS: 111 N. Hill St. MAILING ADDRESS: 111 N. Hill St. CITY AND ZIP CODE: Los Angeles, 90012 BRANCH NAME: Stanley Mosk Courthouse			
CASE NAME: Raffi Kelechian v. Samsung Electronics America, Inc.			
CIVIL CASE COVER SHEET <input checked="" type="checkbox"/> Unlimited (Amount demanded exceeds \$25,000) <input type="checkbox"/> Limited (Amount demanded is \$25,000 or less)		Complex Case Designation <input type="checkbox"/> Counter <input type="checkbox"/> Joinder Filed with first appearance by defendant (Cal. Rules of Court, rule 3.402)	CASE NUMBER: 22STCV30284
		JUDGE: DEPT:	

Items 1–6 below must be completed (see instructions on page 2).

1. Check **one** box below for the case type that best describes this case:

Auto Tort <input type="checkbox"/> Auto (22) <input type="checkbox"/> Uninsured motorist (46) Other PI/PD/WD (Personal Injury/Property Damage/Wrongful Death) Tort <input type="checkbox"/> Asbestos (04) <input type="checkbox"/> Product liability (24) <input type="checkbox"/> Medical malpractice (45) <input type="checkbox"/> Other PI/PD/WD (23) Non-PI/PD/WD (Other) Tort <input checked="" type="checkbox"/> Business tort/unfair business practice (07) <input type="checkbox"/> Civil rights (08) <input type="checkbox"/> Defamation (13) <input type="checkbox"/> Fraud (16) <input type="checkbox"/> Intellectual property (19) <input type="checkbox"/> Professional negligence (25) <input type="checkbox"/> Other non-PI/PD/WD tort (35) Employment <input type="checkbox"/> Wrongful termination (36) <input type="checkbox"/> Other employment (15)	Contract <input type="checkbox"/> Breach of contract/warranty (06) <input type="checkbox"/> Rule 3.740 collections (09) <input type="checkbox"/> Other collections (09) <input type="checkbox"/> Insurance coverage (18) <input type="checkbox"/> Other contract (37) Real Property <input type="checkbox"/> Eminent domain/Inverse condemnation (14) <input type="checkbox"/> Wrongful eviction (33) <input type="checkbox"/> Other real property (26) Unlawful Detainer <input type="checkbox"/> Commercial (31) <input type="checkbox"/> Residential (32) <input type="checkbox"/> Drugs (38) Judicial Review <input type="checkbox"/> Asset forfeiture (05) <input type="checkbox"/> Petition re: arbitration award (11) <input type="checkbox"/> Writ of mandate (02) <input type="checkbox"/> Other judicial review (39)	Provisionally Complex Civil Litigation (Cal. Rules of Court, rules 3.400–3.403) <input type="checkbox"/> Antitrust/Trade regulation (03) <input type="checkbox"/> Construction defect (10) <input type="checkbox"/> Mass tort (40) <input type="checkbox"/> Securities litigation (28) <input type="checkbox"/> Environmental/Toxic tort (30) <input type="checkbox"/> Insurance coverage claims arising from the above listed provisionally complex case types (41) Enforcement of Judgment <input type="checkbox"/> Enforcement of judgment (20) Miscellaneous Civil Complaint <input type="checkbox"/> RICO (27) <input type="checkbox"/> Other complaint (not specified above) (42) Miscellaneous Civil Petition <input type="checkbox"/> Partnership and corporate governance (21) <input type="checkbox"/> Other petition (not specified above) (43)
---	--	--

2. This case ☒ is ☐ is not complex under rule 3.400 of the California Rules of Court. If the case is complex, mark the factors requiring exceptional judicial management:
- | | |
|---|--|
| a. <input type="checkbox"/> Large number of separately represented parties
b. <input type="checkbox"/> Extensive motion practice raising difficult or novel issues that will be time-consuming to resolve
c. <input checked="" type="checkbox"/> Substantial amount of documentary evidence | d. <input checked="" type="checkbox"/> Large number of witnesses
e. <input type="checkbox"/> Coordination with related actions pending in one or more courts in other counties, states, or countries, or in a federal court
f. <input checked="" type="checkbox"/> Substantial postjudgment judicial supervision |
|---|--|
3. Remedies sought (check all that apply): a. ☒ monetary b. ☒ nonmonetary; declaratory or injunctive relief c. ☒ punitive
4. Number of causes of action (specify): 5
5. This case ☒ is ☐ is not a class action suit.
6. If there are any known related cases, file and serve a notice of related case. (You may use form CM-015.)

Date: 09/07/22

Daniel Srourian, Esq.

(TYPE OR PRINT NAME)

(SIGNATURE OF PARTY OR ATTORNEY FOR PARTY)

NOTICE

- Plaintiff must file this cover sheet with the first paper filed in the action or proceeding (except small claims cases or cases filed under the Probate Code, Family Code, or Welfare and Institutions Code). (Cal. Rules of Court, rule 3.220.) Failure to file may result in sanctions.
- File this cover sheet in addition to any cover sheet required by local court rule.
- If this case is complex under rule 3.400 et seq. of the California Rules of Court, you must serve a copy of this cover sheet on all other parties to the action or proceeding.
- Unless this is a collections case under rule 3.740 or a complex case, this cover sheet will be used for statistical purposes only.

Page 1 of 2

INSTRUCTIONS ON HOW TO COMPLETE THE COVER SHEET

To Plaintiffs and Others Filing First Papers. If you are filing a first paper (for example, a complaint) in a civil case, you **must** complete and file, along with your first paper, the *Civil Case Cover Sheet* contained on page 1. This information will be used to compile statistics about the types and numbers of cases filed. You must complete items 1 through 6 on the sheet. In item 1, you must check **one** box for the case type that best describes the case. If the case fits both a general and a more specific type of case listed in item 1, check the more specific one. If the case has multiple causes of action, check the box that best indicates the **primary** cause of action. To assist you in completing the sheet, examples of the cases that belong under each case type in item 1 are provided below. A cover sheet must be filed only with your initial paper. Failure to file a cover sheet with the first paper filed in a civil case may subject a party, its counsel, or both to sanctions under rules 2.30 and 3.220 of the California Rules of Court.

To Parties in Rule 3.740 Collections Cases. A "collections case" under rule 3.740 is defined as an action for recovery of money owed in a sum stated to be certain that is not more than \$25,000, exclusive of interest and attorney's fees, arising from a transaction in which property, services, or money was acquired on credit. A collections case does not include an action seeking the following: (1) tort damages, (2) punitive damages, (3) recovery of real property, (4) recovery of personal property, or (5) a prejudgment writ of attachment. The identification of a case as a rule 3.740 collections case on this form means that it will be exempt from the general time-for-service requirements and case management rules, unless a defendant files a responsive pleading. A rule 3.740 collections case will be subject to the requirements for service and obtaining a judgment in rule 3.740.

To Parties in Complex Cases. In complex cases only, parties must also use the *Civil Case Cover Sheet* to designate whether the case is complex. If a plaintiff believes the case is complex under rule 3.400 of the California Rules of Court, this must be indicated by completing the appropriate boxes in items 1 and 2. If a plaintiff designates a case as complex, the cover sheet must be served with the complaint on all parties to the action. A defendant may file and serve no later than the time of its first appearance a joinder in the plaintiff's designation, a counter-designation that the case is not complex, or, if the plaintiff has made no designation, a designation that the case is complex.

CASE TYPES AND EXAMPLES

Auto Tort

Auto (22)—Personal Injury/Property
Damage/Wrongful Death
Uninsured Motorist (46) (*if the
case involves an uninsured
motorist claim subject to
arbitration, check this item
instead of Auto*)

**Other PI/PD/WD (Personal Injury/
Property Damage/Wrongful Death)
Tort**

Asbestos (04)
Asbestos Property Damage
Asbestos Personal Injury/
Wrongful Death
Product Liability (*not asbestos or
toxic/environmental*) (24)
Medical Malpractice (45)
Medical Malpractice—
Physicians & Surgeons
Other Professional Health Care
Malpractice
Other PI/PD/WD (23)
Premises Liability (e.g., slip
and fall)
Intentional Bodily Injury/PD/WD
(e.g., assault, vandalism)
Intentional Infliction of
Emotional Distress
Negligent Infliction of
Emotional Distress
Other PI/PD/WD

Non-PI/PD/WD (Other) Tort

Business Tort/Unfair Business
Practice (07)
Civil Rights (e.g., discrimination,
false arrest) (*not civil
harassment*) (08)
Defamation (e.g., slander, libel)
(13)
Fraud (16)
Intellectual Property (19)
Professional Negligence (25)
Legal Malpractice
Other Professional Malpractice
(*not medical or legal*)
Other Non-PI/PD/WD Tort (35)

Employment

Wrongful Termination (36)
Other Employment (15)

Contract

Breach of Contract/Warranty (06)
Breach of Rental/Lease
Contract (*not unlawful detainer
or wrongful eviction*)
Contract/Warranty Breach—Seller
Plaintiff (*not fraud or negligence*)
Negligent Breach of Contract/
Warranty
Other Breach of Contract/Warranty
Collections (e.g., money owed, open
book accounts) (09)
Collection Case—Seller Plaintiff
Other Promissory Note/Collections
Case
Insurance Coverage (*not provisionally
complex*) (18)
Auto Subrogation
Other Coverage
Other Contract (37)
Contractual Fraud
Other Contract Dispute

Real Property

Eminent Domain/Inverse
Condemnation (14)
Wrongful Eviction (33)
Other Real Property (e.g., quiet title) (26)
Writ of Possession of Real Property
Mortgage Foreclosure
Quiet Title
Other Real Property (*not eminent
domain, landlord/tenant, or
foreclosure*)

Unlawful Detainer

Commercial (31)
Residential (32)
Drugs (38) (*if the case involves illegal
drugs, check this item; otherwise,
report as Commercial or Residential*)

Judicial Review

Asset Forfeiture (05)
Petition Re: Arbitration Award (11)
Writ of Mandate (02)
Writ—Administrative Mandamus
Writ—Mandamus on Limited Court
Case Matter
Writ—Other Limited Court Case
Review
Other Judicial Review (39)
Review of Health Officer Order
Notice of Appeal—Labor
Commissioner Appeals

**Provisionally Complex Civil Litigation (Cal.
Rules of Court Rules 3.400–3.403)**

Antitrust/Trade Regulation (03)
Construction Defect (10)
Claims Involving Mass Tort (40)
Securities Litigation (28)
Environmental/Toxic Tort (30)
Insurance Coverage Claims
(*arising from provisionally complex
case type listed above*) (41)

Enforcement of Judgment

Enforcement of Judgment (20)
Abstract of Judgment (Out of
County)
Confession of Judgment (*non-
domestic relations*)
Sister State Judgment
Administrative Agency Award
(*not unpaid taxes*)
Petition/Certification of Entry of
Judgment on Unpaid Taxes
Other Enforcement of Judgment
Case

Miscellaneous Civil Complaint

RICO (27)
Other Complaint (*not specified
above*) (42)
Declaratory Relief Only
Injunctive Relief Only (*non-
harassment*)
Mechanics Lien
Other Commercial Complaint
Case (*non-tort/non-complex*)
Other Civil Complaint
(*non-tort/non-complex*)

Miscellaneous Civil Petition

Partnership and Corporate
Governance (21)
Other Petition (*not specified
above*) (43)
Civil Harassment
Workplace Violence
Elder/Dependent Adult
Abuse
Election Contest
Petition for Name Change
Petition for Relief From Late
Claim
Other Civil Petition

SHORT TITLE Raffi Kelechian v. Samsung Electronics America, Inc.	CASE NUMBER 22STCV30284
---	----------------------------

CIVIL CASE COVER SHEET ADDENDUM AND STATEMENT OF LOCATION
(CERTIFICATE OF GROUNDS FOR ASSIGNMENT TO COURTHOUSE LOCATION)

This form is required pursuant to Local Rule 2.3 in all new civil case filings in the Los Angeles Superior Court

Step 1: After completing the Civil Case Cover Sheet (Judicial Council form CM-010), find the exact case type in Column A that corresponds to the case type indicated in the Civil Case Cover Sheet.

Step 2: In Column B, check the box for the type of action that best describes the nature of the case.

Step 3: In Column C, circle the number which explains the reason for the court filing location you have chosen.

Applicable Reasons for Choosing Courthouse Location (Column C)

1. Class Actions must be filed in the Stanley Mosk Courthouse, Central District.	7. Location where petitioner lives.
2. Permissive filing in Central District.	8. Location wherein defendant/respondent functions wholly.
3. Location where cause of action arose.	9. Location where one or more of the parties reside.
4. Mandatory personal injury filing in North District.	10. Location of Labor Commissioner Office.
5. Location where performance required, or defendant resides.	11. Mandatory filing location (Hub Cases – unlawful detainer, limited non-collection, limited collection, or personal injury).
6. Location of property or permanently garaged vehicle.	

	A Civil Case Cover Sheet Case Type	B Type of Action (check only one)	C Applicable Reasons (See Step 3 above)
Personal Injury Cases Assigned to the Personal Injury Hub Courts			
Auto Tort	Auto (22)	<input type="checkbox"/> 2201 Motor Vehicle – Personal Injury/Property Damage/Wrongful Death	1, 4, 11
	Uninsured Motorist (46)	<input type="checkbox"/> 4601 Uninsured Motorist – Personal Injury/Property Damage/Wrongful Death	1, 4, 11
	Other Personal Injury/ Property Damage/ Wrongful Death (23)	<input type="checkbox"/> 2301 Premise Liability (e.g., dangerous conditions of property, slip/trip and fall, dog attack, etc.)	1, 4, 11
		<input type="checkbox"/> 2302 Intentional Bodily Injury/Property Damage/Wrongful Death (e.g., assault, battery, vandalism, etc.)	1, 4, 11
		<input type="checkbox"/> 2303 Intentional Infliction of Emotional Distress	1, 4, 11
		<input type="checkbox"/> 2304 Other Personal Injury/Property Damage/Wrongful Death	1, 4, 11
		<input type="checkbox"/> 2307 Construction Accidents	1, 4, 11

SHORT TITLE Raffi Kelechian v. Samsung Electronics America, Inc.	CASE NUMBER
---	-------------

	A Civil Case Cover Sheet Case Type	B Type of Action (check only one)	C Applicable Reasons (See Step 3 above)
--	--	---	---

Personal Injury Cases Assigned to the Independent Calendar Courts

Other Personal Injury/Property Damage/Wrongful Death Tort	Product Liability (24)	<input type="checkbox"/> 2401 Product Liability (not asbestos or toxic/ environmental)	1, 3, 5
		<input type="checkbox"/> 2402 Product Liability – Song-Beverly Consumer Warranty Act (CA Civil Code §§1790-1795.8) (Lemon Law)	1, 3, 5
	Medical Malpractice (45)	<input type="checkbox"/> 4501 Medical Malpractice – Physicians & Surgeons	1, 3, 5
		<input type="checkbox"/> 4502 Other Professional Health Case Malpractice	1, 3, 5
	Other Personal Injury / Property Damage / Wrongful Death (23)	<input type="checkbox"/> 2305 Elder/Dependent Adult Abuse/Claims Against Skilled Nursing Facility	1, 3, 5
		<input type="checkbox"/> 2306 Intentional Conduct – Sexual Abuse Case (in any form)	1, 3, 5
		<input type="checkbox"/> 2308 Landlord – Tenant Habitability (e.g., bed bugs, mold, etc.)	1, 3, 5

Other Civil Cases Assigned to Independent Calendar Courts

Non-Personal Injury/Property Damage /Wrongful Death Tort	Business Tort (07)	<input checked="" type="checkbox"/> 0701 Other Commercial/Business Tort (not fraud or breach of contract)	1, 2, 3
	Civil Rights (08)	<input type="checkbox"/> 0801 Civil Rights/Discrimination	1, 2, 3
	Defamation (13)	<input type="checkbox"/> 1301 Defamation (slander/libel)	1, 2, 3
	Fraud (16)	<input type="checkbox"/> 1601 Fraud (no contract)	1, 2, 3
	Professional Negligence (25)	<input type="checkbox"/> 2501 Legal Malpractice	1, 2, 3
		<input type="checkbox"/> 2502 Other Professional Malpractice (not medical or legal)	1, 2, 3
	Other (35)	<input type="checkbox"/> 3501 Other Non-Personal Injury/Property Damage Tort	1, 2, 3
Employment	Wrongful Termination (36)	<input type="checkbox"/> 3601 Wrongful Termination	1, 2, 3
	Other Employment (15)	<input type="checkbox"/> 1501 Other Employment Complaint Case	1, 2, 3
		<input type="checkbox"/> 1502 Labor Commissioner Appeals	10
Contract	Breach of Contract / Warranty (06) (not insurance)	<input type="checkbox"/> 0601 Breach of Rental/Lease Contract (not unlawful detainer or wrongful eviction)	2, 5
		<input type="checkbox"/> 0602 Contract/Warranty Breach – Seller Plaintiff (no fraud/negligence)	2, 5
		<input type="checkbox"/> 0603 Negligent Breach of Contract/Warranty (no fraud)	1, 2, 5

SHORT TITLE	Raffi Kelechian v. Samsung Electronics America, Inc.	CASE NUMBER
-------------	--	-------------

	A Civil Case Cover Sheet Case Type	B Type of Action (check only one)	C Applicable Reasons (See Step 3 above)
Contract	Breach of Contract/ Warranty (06) (not insurance)	<input type="checkbox"/> 0604 Other Breach of Contract/Warranty (no fraud/ negligence) <input type="checkbox"/> 0605 Breach of Rental/Lease Contract (COVID-19 Rental Debt)	1, 2, 5 2, 5
	Collections (09)	<input type="checkbox"/> 0901 Collections Case – Seller Plaintiff <input type="checkbox"/> 0902 Other Promissory Note/Collections Case <input type="checkbox"/> 0903 Collections Case – Purchased Debt (charged off consumer debt purchased on or after January 1, 2014) <input type="checkbox"/> 0904 Collections Case – COVID-19 Rental Debt	5, 6, 11 5, 11 5, 6, 11 5, 11
	Insurance Coverage (18)	<input type="checkbox"/> 1801 Insurance Coverage (not complex)	1, 2, 5, 8
	Other Contract (37)	<input type="checkbox"/> 3701 Contractual Fraud	1, 2, 3, 5
		<input type="checkbox"/> 3702 Tortious Interference <input type="checkbox"/> 3703 Other Contract Dispute (not breach/insurance/fraud/ negligence)	1, 2, 3, 5 1, 2, 3, 8, 9
Real Property	Eminent Domain/ Inverse Condemnation (14)	<input type="checkbox"/> 1401 Eminent Domain/Condemnation Number of Parcels _____	2, 6
	Wrongful Eviction (33)	<input type="checkbox"/> 3301 Wrongful Eviction Case	2, 6
	Other Real Property (26)	<input type="checkbox"/> 2601 Mortgage Foreclosure	2, 6
<input type="checkbox"/> 2602 Quiet Title		2, 6	
<input type="checkbox"/> 2603 Other Real Property (not eminent domain, landlord/tenant, foreclosure)		2, 6	
Unlawful Detainer	Unlawful Detainer – Commercial (31)	<input type="checkbox"/> 3101 Unlawful Detainer – Commercial (not drugs or wrongful eviction)	6, 11
	Unlawful Detainer – Residential (32)	<input type="checkbox"/> 3201 Unlawful Detainer – Residential (not drugs or wrongful eviction)	6, 11
	Unlawful Detainer – Post Foreclosure (34)	<input type="checkbox"/> 3401 Unlawful Detainer – Post Foreclosure	2, 6, 11
	Unlawful Detainer – Drugs (38)	<input type="checkbox"/> 3801 Unlawful Detainer – Drugs	2, 6, 11
Judicial Review	Asset Forfeiture (05)	<input type="checkbox"/> 0501 Asset Forfeiture Case	2, 3, 6
	Petition re Arbitration (11)	<input type="checkbox"/> 1101 Petition to Compel/Confirm/Vacate Arbitration	2, 5
	Writ of Mandate (02)	<input type="checkbox"/> 0201 Writ – Administrative Mandamus	2, 8
		<input type="checkbox"/> 0202 Writ – Mandamus on Limited Court Case Matter <input type="checkbox"/> 0203 Writ – Other Limited Court Case Review	2 2

SHORT TITLE Raffi Kelechian v. Samsung Electronics America, Inc.	CASE NUMBER
---	-------------

	A Civil Case Cover Sheet Case Type	B Type of Action (check only one)	C Applicable Reasons (See Step 3 above)
Judicial Review	Other Judicial Review (39)	<input type="checkbox"/> 3901 Other Writ/Judicial Review <input type="checkbox"/> 3902 Administrative Hearing <input type="checkbox"/> 3903 Parking Appeal	2, 8 2, 8 2, 8
Provisionally Complex Litigation	Antitrust/Trade Regulation (03)	<input type="checkbox"/> 0301 Antitrust/Trade Regulation	1, 2, 8
	Asbestos (04)	<input type="checkbox"/> 0401 Asbestos Property Damage <input type="checkbox"/> 0402 Asbestos Personal Injury/Wrongful Death	1, 11 1, 11
	Construction Defect (10)	<input type="checkbox"/> 1001 Construction Defect	1, 2, 3
	Claims Involving Mass Tort (40)	<input type="checkbox"/> 4001 Claims Involving Mass Tort	1, 2, 8
	Securities Litigation (28)	<input type="checkbox"/> 2801 Securities Litigation Case	1, 2, 8
	Toxic Tort Environmental (30)	<input type="checkbox"/> 3001 Toxic Tort/Environmental	1, 2, 3, 8
	Insurance Coverage Claims from Complex Case (41)	<input type="checkbox"/> 4101 Insurance Coverage/Subrogation (complex case only)	1, 2, 5, 8
Enforcement of Judgment	Enforcement of Judgment (20)	<input type="checkbox"/> 2001 Sister State Judgment <input type="checkbox"/> 2002 Abstract of Judgment <input type="checkbox"/> 2003 Confession of Judgment (non-domestic relations) <input type="checkbox"/> 2004 Administrative Agency Award (not unpaid taxes) <input type="checkbox"/> 2005 Petition/Certificate for Entry of Judgment Unpaid Tax <input type="checkbox"/> 2006 Other Enforcement of Judgment Case	2, 5, 11 2, 6 2, 9 2, 8 2, 8 2, 8, 9
Miscellaneous Civil Complaints	RICO (27)	<input type="checkbox"/> 2701 Racketeering (RICO) Case	1, 2, 8
	Other Complaints (not specified above) (42)	<input type="checkbox"/> 4201 Declaratory Relief Only <input type="checkbox"/> 4202 Injunctive Relief Only (not domestic/harassment) <input type="checkbox"/> 4203 Other Commercial Complaint Case (non-tort/non-complex) <input type="checkbox"/> 4304 Other Civil Complaint (non-tort/non-complex)	1, 2, 8 2, 8 1, 2, 8 1, 2, 8
	Partnership Corporation Governance (21)	<input type="checkbox"/> 2101 Partnership and Corporation Governance Case	2, 8
	Other Petitions (not specified above) (43)	<input type="checkbox"/> 4301 Civil Harassment with Damages <input type="checkbox"/> 4302 Workplace Harassment with Damages	2, 3, 9 2, 3, 9

SHORT TITLE Raffi Kelechian v. Samsung Electronics America, Inc.	CASE NUMBER
---	-------------

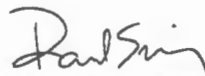
	A Civil Case Cover Sheet Case Type	B Type of Action (check only one)	C Applicable Reasons (See Step 3 above)
Miscellaneous Civil Petitions	Other Petitions (not specified above) (43)	<input type="checkbox"/> 4303 Elder/Dependent Adult Abuse Case with Damages <input type="checkbox"/> 4304 Election Contest <input type="checkbox"/> 4305 Petition for Change of Name/Change of Gender <input type="checkbox"/> 4306 Petition for Relief from Late Claim Law <input type="checkbox"/> 4307 Other Civil Petition	2, 3, 9 2 2, 7 2, 3, 8 2, 9

Step 4: Statement of Reason and Address: Check the appropriate boxes for the numbers shown under Column C for the type of action that you have selected. Enter the address, which is the basis for the filing location including zip code. (No address required for class action cases).

REASON: <input checked="" type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. <input type="checkbox"/> 6. <input type="checkbox"/> 7. <input type="checkbox"/> 8. <input type="checkbox"/> 9. <input type="checkbox"/> 10. <input type="checkbox"/> 11.			ADDRESS:
CITY:	STATE:	ZIP CODE:	

Step 5: Certification of Assignment: I certify that this case is properly filed in the Central District of the Superior Court of California, County of Los Angeles [Code of Civ. Proc., 392 et seq., and LASC Local Rule 2.3(a)(1)(E)]

Dated: 09-07-22



(SIGNATURE OF ATTORNEY/FILING PARTY)

PLEASE HAVE THE FOLLOWING ITEMS COMPLETED AND READY TO BE FILED IN ORDER TO PROPERLY COMMENCE YOUR NEW COURT CASE:

1. Original Complaint or Petition.
2. If filing a Complaint, a completed Summons form for issuance by the Clerk.
3. Civil Case Cover Sheet Judicial Council form CM-010.
4. Civil Case Cover Sheet Addendum and Statement of Location form LASC CIV 109 (05/22).
5. Payment in full of the filing fee, unless there is a court order for waiver, partial or schedule payments.
6. A signed order appointing a Guardian ad Litem, Judicial Council form CIV-010, if the plaintiff or petitioner is a minor under 18 years of age will be required by Court to issue a Summons.
7. Additional copies of documents to be conformed by the Clerk. Copies of the cover sheet and this addendum must be served along with the Summons and Complaint, or other initiating pleading in the case.

SROURIAN LAW FIRM, P.C.
Daniel Srourian, Esq. [SBN 285678]
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: 213.474.3800
Facsimile: 213.471.4160
Email: *daniel@slfla.com*

Attorneys for Plaintiff and the Proposed Class

**SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES**

RAFFI KELECHIAN, individually, and on behalf
of all others similarly situated;

Plaintiff,

v.

SAMSUNG ELECTRONICS AMERICA, INC.,
a New York corporation; and DOES 1 through
100, inclusive;

Defendants.

Case Number: **22STCV30284**

CLASS ACTION COMPLAINT FOR:

- 1. NEGLIGENCE;**
- 2. NEGLIGENCE *PER SE*;**
- 3. BREACH OF IMPLIED CONTRACT;**
- 4. BREACH OF CONFIDENCE;**
- 5. UNFAIR BUSINESS PRACTICES**

DEMAND FOR JURY TRIAL

Plaintiff Raffi Kelechian ("Plaintiffs") brings this Class Action Complaint against Defendant Samsung Electronics America, Inc. ("Samsung") in his individual capacity and on behalf of all others similarly situated (the "Class," defined below), and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

JURISDICTION AND VENUE

1. This Court has jurisdiction over this action under section 410.10 of the California Code of Civil Procedure and Article VI, section 10 of the California Constitution.

2. This Court has personal jurisdiction over Defendant because Defendant conducts business in California and maintains sufficient contacts with the state.

3. Venue is appropriate for the following reasons:

- 1 a. Plaintiff resides in the City of Los Angeles, California, within Los Angeles County,
- 2 California;
- 3 b. the injury to Plaintiff occurred within this judicial district; and,
- 4 c. Defendant conducted business within this judicial district at all relevant times.
- 5 4. Plaintiff is a citizen of Los Angeles County in the State of California.

6 **NATURE OF THE ACTION**

7 5. This class action arises out of the recent targeted cyber-attack against Defendant that
8 allowed a malicious third party to access Defendant's computer systems and data (the "Cyber-
9 Attack"), resulting in the compromise of highly sensitive personal information belonging to
10 millions of Plex users (the "Data Breach").

11 6. As a result of the Cyber-Attack, Plaintiff and Class Members suffered ascertainable
12 injury and damages in the form of the substantial and present risk of fraud and identity theft from
13 their unlawfully accessed and compromised private and confidential information lost value of their
14 private and confidential information, out-of-pocket expenses and the value of their time reasonably
15 incurred to remedy or mitigate the effects of the Cyber-Attack.

16 7. Sensitive personal information of Plaintiff and Class Members— which had been
17 entrusted to Defendant, its officers and agents—was compromised, unlawfully accessed, and stolen
18 due to the Cyber-Attack. Information compromised in the Cyber-Attack includes the following:
19 name, contact and demographic information, date of birth, and product registration information
(collectively, the "Private Information").

20 8. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to
21 address Defendant's inadequate safeguarding of Class Members' Private Information that
22 Defendant collected and maintained.

23 9. Defendant maintained the Private Information in a reckless manner. In particular,
24 Defendant maintained the Private Information Defendant's computer network in a condition
25 vulnerable to cyber-attacks of this type.

26 10. The mechanism of the Cyber-Attack and potential for improper disclosure of
27 Plaintiffs' and Class Members' Private Information was a known and foreseeable risk to
28 Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private
Information from those risks left the Private Information in a dangerous condition.

1 11. Plaintiffs' and Class Members' identities are now at risk because of Defendant's
2 negligent conduct because the Private Information that Defendant collected and maintained is now
3 in the hands of data thieves.

4 12. Armed with the Private Information accessed in the Cyber-Attack, data thieves can
5 commit a variety of crimes against Plaintiff and Class Members, including, *e.g.*, opening new
6 financial accounts in the names of Plaintiff and Class Members; taking out loans in the names of
7 Plaintiff and Class Members; using the Private Information of Plaintiff and Class Members to
8 obtain government benefits; filing fraudulent tax returns using the Private Information of Plaintiff
9 and Class Members; obtaining driver licenses in the names of Plaintiff and Class Members but
10 substituting their photographs with those of other persons; and giving false information to police
11 during an arrest.

12 13. As a further result of the Cyber-Attack, Plaintiff and Class Members have been
13 exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members
14 must now and in the future closely monitor their financial accounts to guard against identity theft.

15 14. Plaintiff and Class Members have and may also incur out of pocket costs for, *e.g.*,
16 purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to
17 deter and detect identity theft.

18 15. As a direct and proximate result of the Cyber-Attack and subsequent Data Breach,
19 Plaintiff and Class Members have suffered and will continue to suffer damages and economic
20 losses in the form of: 1) the loss of time needed to take appropriate measures to avoid unauthorized
21 and fraudulent charges; change their usernames and passwords on their accounts; investigate,
22 correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent
23 to the Data Breach; and 2) charges, and fees charged against their accounts. Plaintiff and Class
24 Members have likewise suffered and will continue to suffer an invasion of their property interest in
25 their own personally identifying information ("PII") such that they are entitled to damages for
26 unauthorized access to and misuse of their PII from Defendant, and Plaintiff and Class Members
27 will suffer from future damages associated with the unauthorized use and misuse of their PII as
28 thieves will continue to use the stolen information to obtain money and credit in their name for
several years.

1 16. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly
2 situated individuals whose Private Information was accessed and/or removed from the network
3 during the Cyber-Attack.

4 17. Plaintiff seeks remedies including, but not limited to, compensatory damages,
5 nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including
6 improvements to Defendant's data security systems, future annual audits, and adequate credit
7 monitoring services funded by Defendant.

8 18. Accordingly, Plaintiff brings this action against Defendant seeking redress for their
9 unlawful conduct asserting claims for negligence, negligence *per se*, and breach of implied
10 contract.

11 **FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS**

12 *Defendant's Business*

13 19. Defendant is a self-proclaimed global streaming media platform with approximately
14 20 million users.

15 20. In the ordinary course of doing business with Defendant, current and former
16 customers provide Defendant with sensitive, personal and private information.

17 21. Plaintiff and Class Members, as current and former customers, relied on Defendant
18 to keep their PII confidential and securely maintained, to use this information for business purposes
19 only, and to make only authorized disclosures of this information. Plaintiff and Class Members
20 demand security to safeguard their PII.

21 22. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and
22 Class Members from involuntary disclosure to third parties.

23 ***The Cyber-Attack and Data Breach***

24 24. On or about September 2, 2022, Defendant began notifying users about the "Data
25 Breach".

26 25. Based on the Notice of Data Breach letters they received, which informed Plaintiff
27 that their Private Information was accessed on Defendant's network and computer systems, and
28 other publicly available information, Plaintiff believes his Private Information was stolen from
Defendant's network and subsequently sold on the dark web.

1 26. Defendant had obligations created by contract, industry standards, common law, and
2 representations made to Plaintiff and Class Members, to keep their Private Information confidential
3 and to protect it from unauthorized access and disclosure.

4 27. Plaintiff and Class Members provided their Private Information to Defendant with
5 the reasonable expectation and mutual understanding that Defendant would comply with its
6 obligations to keep Private information confidential and secure from unauthorized access.

7 28. Defendant's data security obligations were particularly important given the
8 substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

9 29. In 2019, a record 1,473 data breaches occurred, resulting in approximately
10 164,683,455 sensitive records being exposed, a 17% increase from 2018.¹

11 30. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so
12 notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a
13 warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the
14 increase in such attacks, and attendant risk of future attacks, was widely known and completely
15 foreseeable to the public and to anyone in Defendant's industry, including Defendant.

16 ***Plaintiffs' Exposure and Mitigation Efforts***

17 31. As a direct result of the Data Breach, Plaintiff has engaged in mitigation efforts and
18 expended time and resources.

19 32. Subsequent to the Data Breach, Plaintiff subscribed to a credit monitoring service at
20 the cost of \$20 per month.

21 33. Subsequent to the Data Breach, Plaintiff now regularly checks his credit reports as
22 well as his banking statements and credit card statements several times a week. This is time
23 Plaintiff otherwise would have spent performing other activities, such as his working or leisure
24 activities.

25 34. Knowing that thieves stole his PII and knowing that this information may now, or in
26 the future, be available for sale on the dark web has caused Plaintiff. He is now very concerned
27 about identity theft in general. This Data Breach has given Plaintiff hesitation about using
28 electronic services and reservations about conducting other online activities requiring his PII.

¹ https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 10, 2020).

1 35. Prior to receiving the Notice of Data Breach letter from Defendant, Plaintiff had not
2 received a Notice of Data Breach letter from any other company.

3 36. Plaintiff suffered actual injury from having his PII exposed as a result of the Data
4 Breach including, but not limited to: (a) unauthorized credit card charges; (b) entrusting his PII to
5 Defendant which he would not have, had Defendant disclosed that it lacked data security practices
6 adequate to safeguard consumers' PII from theft; (c) damages to and diminution in the value of his
7 PII—a form of intangible property that Plaintiff entrusted to Defendant; (d) loss of his privacy; (e)
8 present injury arising from the increased risk of fraud and identity theft; and (f) the time and
9 expense of his mitigation efforts as a result of the Data Breach.

10 37. As a result of the Data Breach, Plaintiff will continue to be at heightened risk for
11 financial fraud and identity theft, and the attendant damages, for years to come.

12 ***Defendant's Failure to Comply with FTC Guidelines***

13 38. The Federal Trade Commission ("FTC") promulgates numerous guides for
14 businesses highlighting the importance of implementing reasonable data security practices.
15 According to the FTC, the need for data security should be factored into all business decision-
16 making.²

17 39. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide*
18 *for Business*, which established cybersecurity guidelines for businesses.³ The guidelines note that
19 businesses should protect the personal customer information they keep; properly dispose of PII that
20 is no longer needed; encrypt information stored on computer networks; understand their network's
21 vulnerabilities; and implement policies to correct any security problems.

22 40. The FTC further recommends companies not maintain PII longer than is needed for
23 authorization of a transaction; limit access to sensitive data; require complex passwords to be used
24 on networks; use industry-tested methods for security; monitor for suspicious activity on the
25 network; and verify third-party service providers have implemented reasonable security measures.⁴

26 ² Federal Trade Commission, *Start With Security*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed Sept. 9, 2021).

27 ³ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at
28 https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Sept. 9, 2021).

⁴ FTC, *Start With Security*, *supra* note 17.

1 41. The FTC brings enforcement actions against businesses for failing to adequately and
2 reasonably protect customer data, treating the failure to employ reasonable and appropriate
3 measures to protect against unauthorized access to confidential consumer data as an unfair act or
4 practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §
5 45. Orders resulting from these actions further clarify the measures businesses must take to meet
6 their data security obligations.

7 42. Defendant failed to properly implement basic data security practices. Defendant’s
8 failure to employ reasonable and appropriate measures to protect against unauthorized access to
9 members’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15
10 U.S.C. § 45.

11 43. Defendant was at all times fully aware of its obligation to protect Plaintiff and Class
12 Members’ PII. Defendant was also aware of the significant repercussions that would result from its
13 failure to do so.

14 ***Defendant’s Failure to Comply with Industry Standards***

15 44. A number of industry and national best practices have been published and should
16 have been used as a go-to resource and authoritative guide when developing Defendant’s
17 cybersecurity practices.

18 45. Best cybersecurity practices that are standard in the food service industry include
19 installing appropriate malware detection software; monitoring and limiting the network ports;
20 protecting web browsers and email management systems; setting up network systems such as
21 firewalls, switches and routers; monitoring and protection of physical security systems; protection
22 against any possible communication system; training staff regarding critical points.

23 46. Upon information and belief, Defendant failed to meet the minimum standards of
24 the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1
25 (including without limitation PR.AC-1, PR.AC-3, PR.AC- 4, PR.AC-5, PR.AC-6, PR.AC-7,
26 PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT- 3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and
27 RS.CO-2), and the Center for Internet Security’s Critical Security Controls (CIS CSC), which are
28 established standards in reasonable cybersecurity readiness.

1 47. These foregoing frameworks are existing and applicable industry standards in
2 Defendant's industry, and Defendant failed to comply with these accepted standards, thereby
3 opening the door to the Cyber-Attack and causing the data breach.

4 48. ***Defendant's Breach***

5 49. Defendant breached its obligations to Plaintiff and Class Members and/or was
6 otherwise negligent and reckless because it failed to properly maintain and safeguard its computer
7 systems, networks, and data. Defendant's unlawful conduct includes, but is not limited to, the
8 following acts and/or omissions:

- 9 a. Failing to maintain an adequate data security system to reduce the risk of data
10 breaches and cyber-attacks;
- 11 b. Failing to adequately protect Private Information of current and former customers;
- 12 c. Failing to adequately protect current and former customers' Private Information;
- 13 d. Failing to properly monitor its own data security systems for existing intrusions,
14 brute-force attempts, and clearing of event logs;
- 15 e. Failing to apply all available security updates;
- 16 f. Failing to install the latest software patches, update its firewalls, check user account
17 privileges, or ensure proper security practices;
- 18 g. Failing to practice the principle of least-privilege and maintain credential hygiene;
- 19 h. Failing to avoid the use of domain-wide, administrator-level service accounts;
- 20 i. Failing to employ or enforce the use of strong randomized, just-in- time local
21 administrator passwords; and
- 22 j. Failing to properly train and supervise employees in the proper handling of inbound
23 emails.

24 50. As the result of computer systems in need of security upgrading and inadequate
25 procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to
26 safeguard Plaintiff and Class Members' Private Information.

27 ***Data Breaches Put Victims at a Present Increased Risk of***
28 ***Fraud and Identity Theft***

1 51. Defendant understood the Private Information it collected is highly sensitive, and of
2 significant value to those who would use it for wrongful purposes, such as the cyber-criminals who
3 perpetrated this Cyber-Attack.

4 52. The United States Government Accountability Office released a report in 2007
5 regarding data breaches (the “GAO Report”) in which it noted that victims of identity theft will
6 face “substantial costs and time to repair the damage to their good name and credit record.”⁵

7 53. The FTC recommends that identity theft victims take several steps to protect their
8 personal and financial information after a data breach, including contacting one of the credit
9 bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone
10 steals their identity), reviewing their credit reports, contacting companies to remove fraudulent
11 charges from their accounts, placing a credit freeze on their credit, and correcting their credit
12 reports.⁶ Identity thieves use stolen personal information such as Social Security numbers for a
variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

13 54. Identity thieves can also use Social Security numbers to obtain a driver license or
14 official identification card in the victim’s name but with the thief’s picture; use the victim’s name
15 and Social Security number to obtain government benefits; or file a fraudulent tax return using the
16 victim’s information.

17 55. In addition, identity thieves may obtain a job using the victim’s Social Security
18 number, rent a house or receive medical services in the victim’s name, and may even give the
19 victim’s personal information to police during an arrest resulting in an arrest warrant being issued
20 in the victim’s name.

21 56. A study by Identity Theft Resource Center shows the multitude of harms caused by
22 fraudulent use of personal and financial information.⁷

23 57. The value of personal data is axiomatic, considering the value of Big Data in
24 corporate America and the consequences of cyber thefts include heavy prison sentences. Even this
25

26 ⁵ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p.
27 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Apr. 12, 2019) (the
“GAO Report”).

⁶ See <https://www.identitytheft.gov/Steps> (last visited Dec. 8, 2020).

28 ⁷ See Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last accessed Dec. 10, 2020).

1 obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable
2 market value.

3 58. It must also be noted there may be a substantial time lag—measured in years—
4 between when harm occurs versus when it is discovered, and also between when Private
5 Information and/or financial information is stolen and when it is used. According to the U.S.
6 Government Accountability Office, which conducted a study regarding data breaches:

7 59. [L]aw enforcement officials told us that in some cases, stolen data may be held for
8 up to a year or more before being used to commit identity theft. Further, once stolen data have been
9 sold or posted on the Web, fraudulent use of that information may continue for years. As a result,
10 studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out
all future harm. *See* GAO Report at 29.

11 60. Private Information and financial information are such valuable commodities to
12 identity thieves that once the information has been compromised, criminals often trade the
13 information on the “cyber black-market” for years.

14 61. Indeed, a robust “cyber black market” exists in which criminals openly post stolen
15 Private Information on multiple underground Internet websites. Where the most private
16 information belonging to Plaintiff and Class Members was accessed and removed from
17 Defendant’s network, and entire batches of that stolen information already had been dumped by the
18 cyberthieves on the cyber black market, there is a strong probability that additional batches of
19 stolen information are yet to be dumped on the black market, meaning Plaintiff and Class Members
20 are at an increased risk of fraud and identity theft for many years into the future.

21 62. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts
22 for many years to come.

23 63. Sensitive information can sell for as much as \$363 according to the Infosec Institute.
24 PII is particularly valuable because criminals can use it to target victims with frauds and scams.
25 Once PII is stolen, fraudulent use of that information and damage to victims may continue for
years.

26 64. The PII of consumers remains of high value to criminals, as evidenced by the prices
27 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
28 credentials. For example, personal information can be sold at a price ranging from \$40 to \$200.

1 65. Social Security numbers are among the worst kind of personal information to have
2 stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to
3 change. The Social Security Administration stresses that the loss of an individual's Social Security
4 number, as is the case here, can lead to identity theft and extensive financial fraud.

5 66. For example, the Social Security Administration has warned that identity thieves
6 can use an individual's Social Security number to apply for additional credit lines. Such fraud may
7 go undetected until debt collection calls commence months, or even years, later. Stolen Social
8 Security numbers also make it possible for thieves to file fraudulent tax returns, file for
9 unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities
10 is difficult to detect. An individual may not know that his or her Social Security number was used
11 to file for unemployment benefits until law enforcement notifies the individual's employer of the
12 suspected fraud. Fraudulent tax returns are typically discovered only when an individual's
13 authentic tax return is rejected.

14 67. Moreover, it is not an easy task to change or cancel a stolen Social Security number.
15 An individual cannot obtain a new Social Security number without significant paperwork and
16 evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he
17 credit bureaus and banks are able to link the new number very quickly to the old number, so all of
18 that old bad information is quickly inherited into the new Social Security number."⁸

19 68. This data, as one would expect, demands a much higher price on the black market.
20 Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card
21 information, personally identifiable information and Social Security numbers are worth more than
22 10x on the black market."⁹

23 69. At all relevant times, Defendant knew or reasonably should have known these risks,
24 the importance of safeguarding Private Information, and the foreseeable consequences if its data
25 security systems were breached and strengthened their data systems accordingly. Defendant was

26 ⁸ Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Feb. 9, 2015,
<http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last
27 visited Oct. 28, 2020).

28 ⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Feb. 6, 2015,
<http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>
(last visited Oct. 28, 2020).

1 put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to
2 properly prepare for that risk.

3 70. *Plaintiffs' and Class Members' Damages*

4 71. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' PII
5 secure are long lasting and severe. Once that kind of information is stolen, fraudulent use of that
6 information and damage to victims may continue for years. Consumer victims of data breaches are
7 more likely to become victims of identity fraud.¹⁰

8 72. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and
9 left inadequately protected by Defendant—who did not obtain Plaintiffs' or Class Members'
10 consent to disclose such information to any other person as required by applicable law and industry
11 standards.

12 73. The Data Breach was a direct and proximate result of Defendant's failure to: (a)
13 properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use,
14 and disclosure, as required by various state and federal regulations, industry practices, and common
15 law; (b) establish and implement appropriate administrative, technical, and physical safeguards to
16 ensure the security and confidentiality of Plaintiffs' and Class Members' PII; and (c) protect
17 against reasonably foreseeable threats to the security or integrity of such information.

18 74. Defendant had the resources necessary to prevent the Data Breach, but neglected to
19 adequately implement data security measures, despite its obligation to protect member data.

20 75. Defendant could have prevented the intrusions into its systems and, ultimately, the
21 theft of PII if Defendant had remedied the deficiencies in its data security systems and adopted
22 security measures recommended by experts in the field.

23 76. As a direct and proximate result of Defendant's wrongful actions and inactions,
24 Plaintiff and Class Members are now in imminent, immediate, and continuing increased risk of
25 harm from identity theft and fraud, requiring them to dedicate time and resources which they
26 otherwise would have dedicated to other life demands, such as work and family, to mitigate the
27 actual and potential impact of the Data Breach on their lives.

28 ¹⁰ 2014 LexisNexis True Cost of Fraud Study, available at: <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last accessed Sept. 9, 2021)

1 77. The U.S. Department of Justice's Bureau of Justice Statistics found that "among
2 victims who had PII or PHI used for fraudulent purposes, 29% spent a month or more resolving
3 problems," and that "resolving the problems caused by identity theft [could] take more than a year
4 for some victims."¹¹

5 78. In the breach notification letter, Defendant did not much as even make an offer of
6 complementary identity monitoring services to its employees. Victims of data breaches and other
7 unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and
8 financial fraud, and Defendants fail to provide sufficient compensation for the unauthorized release
9 and disclosure of Plaintiffs' and Class Members' PII.

10 79. As a direct result of Defendant's failures to prevent the Data Breach, Plaintiff and
11 Class Members have suffered, will suffer, and are at increased risk of suffering:

- 12 a. The compromise, publication, theft and/or unauthorized use of their PII;
- 13 b. Out-of-pocket costs associated with the prevention, detection, recovery, and
14 remediation from identity theft or fraud;
- 15 c. Lost opportunity costs and lost wages associated with efforts expended and loss of
16 productivity from addressing and attempting to mitigate actual and future
17 consequences of the Data Breach, including but not limited to researching how to
18 prevent, detect, contest, and recover from identity theft and fraud;
- 19 d. The present and continued risk to their PII, which remains in the possession of
20 Defendant and is subject to further breaches so long as Defendant fails to undertake
21 appropriate measures to protect the PII in its possession; and
- 22 e. Current and future costs in terms of time, effort, and money that will be expended to
23 prevent, detect, contest, remediate, and repair the impact of the Data Breach for the
24 remainder of the lives of Plaintiff and Class Members.

25 80. In addition to a remedy for the economic harm, Plaintiff and Class Members
26 maintain an undeniable interest in ensuring their PII is secure, remains secure, and is not subject to
27 further misappropriation and theft.

28 ¹¹ U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft*, 2012, December 2013, available at: <https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last accessed Sept. 9, 2021).

1 81. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and
2 Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an
3 increased risk of future harm.

4 **CLASS ACTION ALLEGATIONS**

5 82. Plaintiff brings this suit on behalf of themselves and a class of similarly situated
6 individuals that are preliminarily defined as:

7
8 All individuals whose PII was compromised in the data breach announced by Samsung on
9 September 2, 2022, who reside in the State of California.

10 83. Excluded from the Class are the following individuals and/or entities: Defendant
11 and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former
12 employees, and any entity in which Defendant has a controlling interest; all individuals who make
13 a timely election to be excluded from this proceeding using the correct protocol for opting out; any
14 and all federal, state or local governments, including but not limited to their departments, agencies,
15 divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; Class counsel; and all
16 judges assigned to hear any aspect of this litigation, as well as their staff and immediate family
17 members.

18 84. Plaintiff reserves the right to modify or amend the definition of the proposed Class
19 before the Court determines whether certification is appropriate.

20 85. **Numerosity:** The Class is so numerous that joinder of all members is impracticable.
21 Defendant has identified more than 100 persons whose PII may have been improperly accessed in
22 the Data Breach, and the Class is identifiable within Defendant's records. A precise number of
23 class members can be ascertained through appropriate discovery and from records maintained by
24 Defendant.

25 86. **Commonality and Predominance:** Questions of law and fact common to the Class
26 exist and predominate over any questions affecting only individual Class members. These include
27 but are not limited to, the following:

- 28 a. Whether Plaintiffs' and the Class members' PII was accessed and/or viewed by one
or more unauthorized persons in the Data Breach alleged above;

- b. Whether Defendant's publishing Plaintiffs' and Class members' PII to unauthorized persons was permissible without the prior written authorization of the Plaintiff or the Class members;
- c. When and how Defendant should have learned and actually learned of the Data Breach;
- d. Whether Defendant's response to the Data Breach was adequate;
- e. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;
- f. Whether Defendant breached that duty;
- g. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class members' PII;
- h. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class members' PII;
- i. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII secure and prevent loss or misuse of that PII;
- j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- k. Whether Defendant caused Plaintiff and Class members damages;
- l. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their PII was compromised;
- m. Whether Plaintiff and Class members are entitled to actual damages, nominal and/or statutory damages, credit monitoring, other monetary relief, and/or equitable relief; and
- n. Whether Defendant violated the California Unfair Competition Law (Business & Professions Code § 17200 *et seq.*).

87. There are no defenses of a unique nature that may be asserted against the Plaintiff individually, as distinguished from the other Class Members, and the relief sought is common to the Class.

1 88. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because
2 all had their PII compromised because of the Data Breach, due to Defendant's identical conduct.

3 89. **Adequacy of Representation:** Plaintiff will fairly and adequately represent and
4 protect the interests of the Class Members in that Plaintiffs' interests are aligned with the class.
5 Plaintiff have no disabling conflicts of interest that would be antagonistic to those of the other
6 members of the Class. Plaintiff seeks no relief that is adverse to Class Members. In addition,
7 Plaintiff retained counsel experienced in data breach and complex consumer class action litigation.
8 Neither Plaintiff nor their counsel have any interests which might cause them not to vigorously
9 pursue this claim.

10 90. **Superiority:** Class action treatment is superior to all other available methods for the
11 fair and efficient adjudication of the controversy alleged herein; it will permit a large number of
12 class members to prosecute their common claims in a single forum simultaneously, efficiently, and
13 without the unnecessary duplication of evidence, effort, and expense that hundreds of individual
14 actions would require. Class action treatment will permit the adjudication of relatively modest
15 claims by certain class members, who could not individually afford to litigate a complex claim
16 against large entities, such as Defendant. Further, even for those Class Members who could afford
17 to litigate such a claim, it would still be economically impractical and impose a burden on the
18 courts.

19 91. The prosecution of separate actions by individual members of the Class would
20 create a risk of inconsistent or varying adjudications with respect to individual members of the
21 Class, and a risk that any adjudications with respect to individual members of the Class would, as a
22 practical matter, either be dispositive of the interests of other members of the Class not party to the
23 adjudication or substantially impair or impede their ability to protect their interests.

24 92. Class certification is also warranted for purposes of injunctive and declaratory relief
25 because Defendant has acted, or refused to act, on grounds generally applicable to the class, so that
26 final injunctive and declaratory relief are appropriate with respect to the Class as a whole.

27 **CLAIMS FOR RELIEF**

28 **First Claim for Relief**

Negligence

(On Behalf of Plaintiff and the Class)

1 93. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set
2 forth herein.

3 94. Defendant's own negligent conduct created a foreseeable risk of harm to Plaintiff
4 and Class Members. Defendant's negligence included, but was not limited to, its failure to take the
5 steps and opportunities to prevent the Data Breach as set forth herein. Defendant's negligence also
6 included its decision not to comply with

7 (1) industry standards, and/or best practices for the safekeeping and encrypted authorized
8 disclosure of the PII of Plaintiff and Class Members; or (2) Section 5 of the FTC Act.

9 95. First, Defendant had a duty to exercise reasonable care in safeguarding, securing
10 and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to
11 unauthorized parties. This duty includes, among other things, designing, maintaining and testing its
12 security protocols to ensure PII in Defendant's possession was adequately secured and protected,
13 and that employees tasked with maintaining such information were adequately trained on relevant
14 cybersecurity measures. Defendant also had a duty to put proper procedures in place to prevent the
15 unauthorized dissemination of Plaintiffs' and Class Members' PII.

16 96. As a condition of employment, Plaintiff and Class Members were obligated to
17 provide Defendant with their PII. As such, Plaintiff and the Class Members entrusted their PII to
18 Defendant with the understanding Defendant would safeguard their information.

19 97. Defendant was in a position to protect against the harm suffered by Plaintiff and
20 Class Members as a result of the Data Breach. However, Plaintiff and Class Members had no
21 ability to protect their PII in Defendant's possession.

22 98. Defendant had full knowledge of the sensitivity of the PII, and the types of harm
23 Plaintiff and Class Members could, would, and will suffer if the information were wrongfully
24 disclosed.

25 99. Defendant admitted that its computer system containing Plaintiffs' and Class
26 Members' PII was wrongfully compromised and accessed by unauthorized third persons, and that
27 the Data Breach occurred due to Defendant's actions and/or omissions.

28 100. Plaintiff and Class Members were the foreseeable and probable victims of
Defendant's negligent and inadequate security practices and procedures that led to the Data Breach.
Defendant knew or should have known of the inherent risks in collecting and storing the highly

1 valuable PII of Plaintiff and Class Members, the critical importance of providing adequate security
2 of that information, the current cyber security risks being perpetrated, and that Defendant had
3 inadequate employee training, monitoring and education and IT security protocols in place to
4 secure the PII of Plaintiff and Class Members.

5 101. Defendant negligently, through its actions and/or omissions, and unlawfully
6 breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in
7 protecting and safeguarding Plaintiffs' and Class Members' PII while the information was within
8 Defendant's possession and/or control by failing to comply with and/or deviating from standard
9 industry rules, regulations, and practices at the time of the Data Breach.

10 102. Second, Defendant's violations of Section 5 of the FTC Act constitute negligence.
11 Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as
12 interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of
13 failing to use reasonable measures to protect PII. The FTC publications and orders described above
14 also form part of the basis of Defendant's duty in this regard.

15 103. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures
16 to protect Plaintiffs' and Class members' PII and not complying with applicable industry standards,
17 as described in detail herein. Defendant's conduct was particularly unreasonable given the nature
18 and amount of PII it required, obtained, and stored, and the foreseeable consequences of a data
19 breach including, specifically, the damages that would result to Plaintiff and Class members.

20 104. Plaintiff and Class Members are within the class of persons the FTC Act was
21 intended to protect.

22 105. The harm the Data Breach caused, and continues to cause, is the type of harm the
23 FTC Act was intended to guard against. The FTC pursues enforcement actions against businesses,
24 which, as a result of their failure to employ reasonable data security measures and avoid unfair and
25 deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

26 106. Defendant, through its actions and/or omissions, unlawfully breached its duty to
27 Plaintiff and Class Members by failing to have appropriate procedures in place to detect and
28 prevent unauthorized dissemination of Plaintiffs' and Class Members' PII.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to
adequately disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

1 108. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and
2 Class Members, Plaintiffs' and Class Members' PII would not have been compromised.

3 109. There is a temporal and close causal connection between Defendant's failure to
4 implement security measures to protect the PII and the harm suffered, and/or risk of present and
5 continual harm suffered, by Plaintiff and Class Members.

6 110. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
7 Members have suffered, and continue to suffer, injuries and damages arising from the Data Breach,
8 including, but not limited to: damages from lost time and efforts to mitigate the actual and potential
9 impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts"
10 with credit reporting agencies, contacting their financial institutions, closely reviewing and
11 monitoring their credit reports and various accounts for unauthorized activity, filing police reports,
12 and damages from identity theft, which may take months—if not years—to discover, detect, and
13 remedy.

14 111. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff
15 and Class Members have suffered, and will continue to suffer, the continued risks of exposure of
16 their PII, which remains in Defendant's possession and is subject to further unauthorized
17 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
18 the PII in its continued possession.

19 **Second Claim for Relief**

20 **Negligence *Per Se***

21 **(On Behalf of Plaintiff and the Class)**

22 112. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set
23 forth herein.

24 113. Pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45, Defendant had a duty to
25 provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and
26 Class Members' Private Information.

27 114. Plaintiff and Class Members are within the class of persons that the FTC Act was
28 intended to protect.

115. The harm that occurred as a result of the Data Breach is the type of harm the FTC
Act was intended to guard against. The FTC has pursued enforcement actions against businesses,

1 which, as a result of their failure to employ reasonable data security measures and avoid unfair and
2 deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

3 116. Defendant breached its duties to Plaintiff and Class Members under the Federal
4 Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and
5 data security practices to safeguard Plaintiffs' and Class Members' Private Information.

6 117. Defendant's failure to comply with applicable laws and regulations constitutes
7 negligence *per se*.

8 118. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff
9 and Class Members, Plaintiff and Class Members would not have been injured.

10 119. The injury and harm suffered by Plaintiff and Class Members was the reasonably
11 foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it
12 was failing to meet their duties, and that Defendant's breach would cause Plaintiff and Class
13 Members to experience the foreseeable harms associated with the exposure of their Private
14 Information.

15 120. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and
16 Class Members have suffered injury and are entitled to compensatory, consequential, and punitive
17 damages in an amount to be proven at trial.

18 **Third Claim for Relief**

19 **Breach of Implied Contract**

20 **(On Behalf of Plaintiff and the Class)**

21 121. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set
22 forth herein.

23 122. Plaintiff and Class Members were required to provide their PII to Defendant as a
24 condition of purchase.

25 123. Plaintiff and Class Members provided their PII to Defendant in exchange for
26 products/services, along with Defendant's promise to protect their PII from unauthorized
27 disclosure.

28 124. Upon information and belief, in its written privacy policies, Defendant expressly
promised Plaintiff and Class Members that it would only disclose PII under certain circumstances,
none of which relate to the Data Breach.

1 125. 135. Implicit in the agreement between Plaintiff and Class Members on the one
2 hand, and Defendant on the other, regarding providing PII, was Defendant's obligation to: (a) use
3 such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent
4 unauthorized disclosures of the PII; (d) provide Plaintiff and Class Members with prompt and
5 sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably
6 safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses;
7 and (f) retain the PII only under conditions that kept such information secure and confidential.

8 126. Without such implied contracts, Plaintiff and Class Members would not have
9 provided their PII to Defendant.

10 127. Plaintiff and Class Members fully performed their obligations under the implied
11 contract with Defendant. However, Defendant did not.

12 128. Defendant breached the implied contracts with Plaintiff and Class members by
13 failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII, which was
14 compromised as a result of the Data Breach.

15 129. As a direct and proximate result of Defendant's breach of the implied contracts,
16 Plaintiff and Class Members have suffered, and continue to suffer, injuries and damages arising
17 from the Data Breach including, but not limited to: damages from lost time and effort to mitigate
18 the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing
19 "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing
20 or modifying financial accounts, closely reviewing and monitoring their credit reports and various
21 accounts for unauthorized activity, filing police reports, and damages from identity theft, which
22 may take months if not years to discover, detect, and remedy.

23 **Fourth Claim for Relief**

24 **Breach of Confidence**

25 **(On Behalf of Plaintiff and the Class)**

26 130. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set
27 forth herein.

28 131. At all times during Plaintiffs' and Class Members' interactions with Defendant,
Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class
Members' PII that Plaintiff and Class Members provided to Defendant.

1 132. As alleged herein and above, Defendant's relationship with Plaintiff and Class
2 Members was governed by terms and expectations that Plaintiffs' and Class Members' PII would
3 be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third
4 parties.

5 133. Plaintiff and Class Members provided their respective PII to Defendant with the
6 explicit and implicit understandings that Defendant would protect and not permit the information to
7 be disseminated to any unauthorized parties.

8 134. Plaintiff and Class Members also provided their PII to Defendant with the explicit
9 and implicit understandings that Defendant would take precautions to protect that PII from
10 unauthorized disclosure, such as following basic principles of protecting its networks and data
11 systems.

12 135. Defendant required and voluntarily received, in confidence, Plaintiffs' and Class
13 Members' PII with the understanding that the information would not be disclosed or disseminated
14 to the public or any unauthorized third parties.

15 136. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from
16 occurring by, *inter alia*, following best information security practices to secure Plaintiffs' and
17 Class Members' PII, Plaintiffs' and Class Members' PII was disclosed to, and misappropriated by,
18 unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their
19 express permission.

20 137. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff
21 and Class Members have suffered, and will continue to suffer damages.

22 138. But for Defendant's disclosure of Plaintiffs' and Class Members' PII in violation of
23 the parties' understanding of confidence, Plaintiffs' and Class Members' PII would not have been
24 compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data
25 Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as
26 the resulting damages.

27 139. The injury and harm Plaintiff and Class Members suffered, and continue to suffer,
28 was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and
Class Members' PII. Defendant knew its computer systems and technologies for accepting and

1 securing Plaintiffs' and Class Members' PII had numerous security and other vulnerabilities
2 placing Plaintiffs' and Class Members' PII in jeopardy.

3 140. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff
4 and Class Members have suffered and will suffer injury, including but not limited to: (a) actual
5 identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses
6 associated with the prevention, detection, and recovery from identity theft and/or unauthorized use
7 of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity
8 addressing and attempting to mitigate the actual and future consequences of the Data Breach,
9 including but not limited to efforts spent researching how to prevent, detect, contest, and recover
10 from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and
11 is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate
12 and adequate measures to protect the PII in its continued possession; (f) future costs in terms of
13 time, effort, and money that will be expended as result of the Data Breach for the remainder of the
14 lives of Plaintiff and Class Members; and (g) the diminished value of Defendant's services they
15 received.

16 141. As a direct and proximate result of Defendant's breaches of its fiduciary duties,
17 Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or
18 harm, and other economic and non-economic losses.

19 **Fifth Claim for Relief**

20 **Violation of the California Unfair Competition Law,**

21 **Cal. Bus. & Prof. Code § 17200 *et seq.*--Unfair Business Practices**

22 **(On Behalf of Plaintiff and the Class)**

23 142. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set
24 forth herein.

25 143. Defendant violated California Unfair Competition Law, Cal. Bus. & Prof. Code §
26 17200 *et seq.* ("UCL"), by engaging in unlawful, unfair, or fraudulent business acts and practices,
27 and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition"
28 as defined in Cal. Bus. & Prof. Code § 17200 with respect to the services provided to Plaintiff and
California Subclass Members.

1 144. Defendant engaged in unlawful acts and practices with respect to the services by
2 establishing the sub-standard security practices and procedures described herein; by soliciting and
3 collecting Plaintiff and California Subclass Members' PII with knowledge the information would
4 not be adequately protected; and by storing Plaintiffs' and California Subclass Members' PII in an
5 unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code §
6 1798.81.5, which require Defendant to take reasonable methods of safeguarding the PII of Plaintiff
7 and California Subclass Members.

8 145. In addition, Defendant engaged in unlawful acts and practices by failing to disclose
9 the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code
10 § 1798.82.

11 146. As a direct and proximate result of Defendant's unlawful practices and acts,
12 Plaintiff and California Subclass Members were injured and lost money or property, including but
13 not limited to the price received by Defendant for the services, the loss of Plaintiff and California
14 Subclass Members' legally protected interest in the confidentiality and privacy of their PII,
15 nominal damages, and additional losses as described herein.

16 147. Defendant knew or should have known Defendant's computer systems and data
17 security practices were inadequate to safeguard Plaintiff and California Subclass Members' PII and
18 that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the
19 above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and
20 reckless with respect to the rights of Plaintiff and the California Subclass Members.

21 148. Plaintiff, on behalf of the California Subclass, seeks relief under the UCL,
22 including, but not limited to, restitution to Plaintiff and California Subclass Members of money or
23 property Defendant may have acquired by means of Defendant's unlawful, and unfair business
24 practices, restitutionary disgorgement of all monies that accrued to Defendant because of
25 Defendant's unlawful and unfair business practices, declaratory relief, attorney fees and costs
26 (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

27 **PRAYER FOR RELIEF**

28 **WHEREFORE**, Plaintiffs, on behalf of themselves and all Class Members, request that the
Court grant judgment against Defendant as follows:

- a. An order certifying the Class as defined herein, and appointing Plaintiff and their Counsel to represent the Class;
- b. Injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein,
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws,
 - iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members,
 - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members,
 - v. prohibiting Defendant from maintaining Plaintiffs' and Class Members' PII on a cloud-based database,
 - vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,
 - vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring,
 - viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures,

- ix. requiring Defendant to conduct regular database scanning and securing checks,
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members,
- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,
- xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII,
- xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,
- xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves,
- xv. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected,
- xvi. requiring Defendant disclose any future data disclosures in a timely and accurate manner; and
- xvii. requiring Defendant to provide ongoing credit monitoring and identity theft repair services to Class Members.

- 1 c. An award of compensatory, statutory, and nominal damages in an amount to be
2 determined;
3 d. An award for equitable relief requiring restitution and disgorgement of the revenues
4 wrongfully retained as a result of Defendant's wrongful conduct;
5 e. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable
6 by law; and
7 f. Such other and further relief as this Court may deem just and proper.

8 **DEMAND FOR JURY TRIAL**

9 Plaintiff hereby demands a trial by jury.

SROURIAN LAW FIRM, PC

10 

11 DATED: September 16, 2022

12 By: _____
13 Daniel Srourian, Esq.
14 Attorney for Plaintiff and the
15 [Proposed] Class
16
17
18
19
20
21
22
23
24
25
26
27
28

SROURIAN LAW FIRM, P.C.
Daniel Srourian, Esq. [SBN 285678]
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: 213.474.3800
Facsimile: 213.471.4160
Email: *daniel@slfla.com*

FILED
Superior Court of California
County of Los Angeles

10/18/2022

By *K. Martinez* Deputy

Attorneys for Plaintiff and the Proposed Class

**SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES**

RAFFI KELECHIAN, individually, and on behalf
of all others similarly situated;

Plaintiff,

v.

SAMSUNG ELECTRONICS AMERICA, INC.,
a New York corporation; and DOES 1 through
100, inclusive;

Defendants.

Case Number: 22STCV30284

*(Assigned for all Purposes to Hon. Elihu Berle,
Department 6)*

FIRST AMENDED COMPLAINT

- 1. NEGLIGENCE;**
- 2. NEGLIGENCE *PER SE*;**
- 3. BREACH OF IMPLIED
CONTRACT;**
- 4. BREACH OF CONFIDENCE;**
- 5. UNFAIR BUSINESS PRACTICES**
- 6. VIOLATION OF CCPA,
CALIFORNIA CIVIL CODE
SECTION 1798.150**

Plaintiff Raffi Kelechian ("Plaintiffs") brings this Class Action Complaint against Defendant Samsung Electronics America, Inc. ("Samsung") in his individual capacity and on behalf of all others similarly situated (the "Class," defined below), and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

JURISDICTION AND VENUE

1. This Court has jurisdiction over this action under section 410.10 of the California Code of Civil Procedure and Article VI, section 10 of the California Constitution.

2. This Court has personal jurisdiction over Defendant because Defendant conducts business in California and maintains sufficient contacts with the state.

1 3. Venue is appropriate for the following reasons:

- 2 a. Plaintiff resides in the City of Los Angeles, California, within Los Angeles County,
3 California;
4 b. the injury to Plaintiff occurred within this judicial district; and,
5 c. Defendant conducted business within this judicial district at all relevant times.

6 4. Plaintiff is a citizen of Los Angeles County in the State of California.

7 **NATURE OF THE ACTION**

8 5. This class action arises out of the recent targeted cyber-attack against Defendant that
9 allowed a malicious third party to access Defendant's computer systems and data (the "Cyber-
10 Attack"), resulting in the compromise of highly sensitive personal information belonging to
11 millions of Plex users (the "Data Breach").

12 6. As a result of the Cyber-Attack, Plaintiff and Class Members suffered ascertainable
13 injury and damages in the form of the substantial and present risk of fraud and identity theft from
14 their unlawfully accessed and compromised private and confidential information lost value of their
15 private and confidential information, out-of-pocket expenses and the value of their time reasonably
16 incurred to remedy or mitigate the effects of the Cyber-Attack.

17 7. Sensitive personal information of Plaintiff and Class Members— which had been
18 entrusted to Defendant, its officers and agents—was compromised, unlawfully accessed, and stolen
19 due to the Cyber-Attack. Information compromised in the Cyber-Attack includes the following:
20 name, contact and demographic information, date of birth, and product registration information
(collectively, the "Private Information").

21 8. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to
22 address Defendant's inadequate safeguarding of Class Members' Private Information that
23 Defendant collected and maintained.

24 9. Defendant maintained the Private Information in a reckless manner. In particular,
25 Defendant maintained the Private Information Defendant's computer network in a condition
26 vulnerable to cyber-attacks of this type.

27 10. The mechanism of the Cyber-Attack and potential for improper disclosure of
28 Plaintiffs' and Class Members' Private Information was a known and foreseeable risk to

1 Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private
2 Information from those risks left the Private Information in a dangerous condition.

3 11. Plaintiffs' and Class Members' identities are now at risk because of Defendant's
4 negligent conduct because the Private Information that Defendant collected and maintained is now
5 in the hands of data thieves.

6 12. Armed with the Private Information accessed in the Cyber-Attack, data thieves can
7 commit a variety of crimes against Plaintiff and Class Members, including, *e.g.*, opening new
8 financial accounts in the names of Plaintiff and Class Members; taking out loans in the names of
9 Plaintiff and Class Members; using the Private Information of Plaintiff and Class Members to
10 obtain government benefits; filing fraudulent tax returns using the Private Information of Plaintiff
11 and Class Members; obtaining driver licenses in the names of Plaintiff and Class Members but
12 substituting their photographs with those of other persons; and giving false information to police
during an arrest.

13 13. As a further result of the Cyber-Attack, Plaintiff and Class Members have been
14 exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members
15 must now and in the future closely monitor their financial accounts to guard against identity theft.

16 14. Plaintiff and Class Members have and may also incur out of pocket costs for, *e.g.*,
17 purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to
18 deter and detect identity theft.

19 15. As a direct and proximate result of the Cyber-Attack and subsequent Data Breach,
20 Plaintiff and Class Members have suffered and will continue to suffer damages and economic
21 losses in the form of: 1) the loss of time needed to take appropriate measures to avoid unauthorized
22 and fraudulent charges; change their usernames and passwords on their accounts; investigate,
23 correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent
24 to the Data Breach; and 2) charges, and fees charged against their accounts. Plaintiff and Class
25 Members have likewise suffered and will continue to suffer an invasion of their property interest in
26 their own personally identifying information ("PII") such that they are entitled to damages for
27 unauthorized access to and misuse of their PII from Defendant, and Plaintiff and Class Members
28 will suffer from future damages associated with the unauthorized use and misuse of their PII as

1 thieves will continue to use the stolen information to obtain money and credit in their name for
2 several years.

3 16. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly
4 situated individuals whose Private Information was accessed and/or removed from the network
5 during the Cyber-Attack.

6 17. Plaintiff seeks remedies including, but not limited to, compensatory damages,
7 nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including
8 improvements to Defendant's data security systems, future annual audits, and adequate credit
9 monitoring services funded by Defendant.

10 18. Accordingly, Plaintiff brings this action against Defendant seeking redress for their
11 unlawful conduct asserting claims for negligence, negligence *per se*, and breach of implied
12 contract.

13 **FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS**

14 *Defendant's Business*

15 19. Defendant is a self-proclaimed global streaming media platform with approximately
16 20 million users.

17 20. In the ordinary course of doing business with Defendant, current and former
18 customers provide Defendant with sensitive, personal and private information.

19 21. Plaintiff and Class Members, as current and former customers, relied on Defendant
20 to keep their PII confidential and securely maintained, to use this information for business purposes
21 only, and to make only authorized disclosures of this information. Plaintiff and Class Members
22 demand security to safeguard their PII.

23 22. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and
24 Class Members from involuntary disclosure to third parties.

25 *23. The Cyber-Attack and Data Breach*

26 24. On or about September 2, 2022, Defendant began notifying users about the "Data
27 Breach".

28 25. Based on the Notice of Data Breach letters they received, which informed Plaintiff
that their Private Information was accessed on Defendant's network and computer systems, and

1 other publicly available information, Plaintiff believes his Private Information was stolen from
2 Defendant's network and subsequently sold on the dark web.

3 26. Defendant had obligations created by contract, industry standards, common law, and
4 representations made to Plaintiff and Class Members, to keep their Private Information confidential
5 and to protect it from unauthorized access and disclosure.

6 27. Plaintiff and Class Members provided their Private Information to Defendant with
7 the reasonable expectation and mutual understanding that Defendant would comply with its
8 obligations to keep Private information confidential and secure from unauthorized access.

9 28. Defendant's data security obligations were particularly important given the
10 substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

11 29. In 2019, a record 1,473 data breaches occurred, resulting in approximately
12 164,683,455 sensitive records being exposed, a 17% increase from 2018.¹

13 30. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so
14 notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a
15 warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the
16 increase in such attacks, and attendant risk of future attacks, was widely known and completely
17 foreseeable to the public and to anyone in Defendant's industry, including Defendant.

18 *Plaintiffs' Exposure and Mitigation Efforts*

19 31. As a direct result of the Data Breach, Plaintiff has engaged in mitigation efforts and
20 expended time and resources.

21 32. Subsequent to the Data Breach, Plaintiff subscribed to a credit monitoring service at
22 the cost of \$20 per month.

23 33. Subsequent to the Data Breach, Plaintiff now regularly checks his credit reports as
24 well as his banking statements and credit card statements several times a week. This is time
25 Plaintiff otherwise would have spent performing other activities, such as his working or leisure
26 activities.

27 34. Knowing that thieves stole his PII and knowing that this information may now, or in
28 the future, be available for sale on the dark web has caused Plaintiff. He is now very concerned

¹ https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 10, 2020).

1 about identity theft in general. This Data Breach has given Plaintiff hesitation about using
2 electronic services and reservations about conducting other online activities requiring his PII.

3 35. Prior to receiving the Notice of Data Breach letter from Defendant, Plaintiff had not
4 received a Notice of Data Breach letter from any other company.

5 36. Plaintiff suffered actual injury from having his PII exposed as a result of the Data
6 Breach including, but not limited to: (a) unauthorized credit card charges; (b) entrusting his PII to
7 Defendant which he would not have, had Defendant disclosed that it lacked data security practices
8 adequate to safeguard consumers' PII from theft; (c) damages to and diminution in the value of his
9 PII—a form of intangible property that Plaintiff entrusted to Defendant; (d) loss of his privacy; (e)
10 present injury arising from the increased risk of fraud and identity theft; and (f) the time and
11 expense of his mitigation efforts as a result of the Data Breach.

12 37. As a result of the Data Breach, Plaintiff will continue to be at heightened risk for
13 financial fraud and identity theft, and the attendant damages, for years to come.

14 ***Defendant's Failure to Comply with FTC Guidelines***

15 38. The Federal Trade Commission ("FTC") promulgates numerous guides for
16 businesses highlighting the importance of implementing reasonable data security practices.
17 According to the FTC, the need for data security should be factored into all business decision-
18 making.²

19 39. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide*
20 *for Business*, which established cybersecurity guidelines for businesses.³ The guidelines note that
21 businesses should protect the personal customer information they keep; properly dispose of PII that
22 is no longer needed; encrypt information stored on computer networks; understand their network's
23 vulnerabilities; and implement policies to correct any security problems.

24 40. The FTC further recommends companies not maintain PII longer than is needed for
25 authorization of a transaction; limit access to sensitive data; require complex passwords to be used
26

27 ² Federal Trade Commission, *Start With Security*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed Sept. 9, 2021).

28 ³ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at
https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Sept. 9, 2021).

1 on networks; use industry-tested methods for security; monitor for suspicious activity on the
2 network; and verify third-party service providers have implemented reasonable security measures.⁴

3 41. The FTC brings enforcement actions against businesses for failing to adequately and
4 reasonably protect customer data, treating the failure to employ reasonable and appropriate
5 measures to protect against unauthorized access to confidential consumer data as an unfair act or
6 practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §
7 45. Orders resulting from these actions further clarify the measures businesses must take to meet
8 their data security obligations.

9 42. Defendant failed to properly implement basic data security practices. Defendant's
10 failure to employ reasonable and appropriate measures to protect against unauthorized access to
11 members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15
12 U.S.C. § 45.

13 43. Defendant was at all times fully aware of its obligation to protect Plaintiff and Class
14 Members' PII. Defendant was also aware of the significant repercussions that would result from its
15 failure to do so.

16 ***Defendant's Failure to Comply with Industry Standards***

17 44. A number of industry and national best practices have been published and should
18 have been used as a go-to resource and authoritative guide when developing Defendant's
19 cybersecurity practices.

20 45. Best cybersecurity practices that are standard in the food service industry include
21 installing appropriate malware detection software; monitoring and limiting the network ports;
22 protecting web browsers and email management systems; setting up network systems such as
23 firewalls, switches and routers; monitoring and protection of physical security systems; protection
24 against any possible communication system; training staff regarding critical points.

25 46. Upon information and belief, Defendant failed to meet the minimum standards of
26 the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1
27 (including without limitation PR.AC-1, PR.AC-3, PR.AC- 4, PR.AC-5, PR.AC-6, PR.AC-7,
28 PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT- 3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and

⁴ FTC, *Start With Security*, *supra* note 17.

1 RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are
2 established standards in reasonable cybersecurity readiness.

3 47. These foregoing frameworks are existing and applicable industry standards in
4 Defendant's industry, and Defendant failed to comply with these accepted standards, thereby
5 opening the door to the Cyber-Attack and causing the data breach.

6 48. ***Defendant's Breach***

7 49. Defendant breached its obligations to Plaintiff and Class Members and/or was
8 otherwise negligent and reckless because it failed to properly maintain and safeguard its computer
9 systems, networks, and data. Defendant's unlawful conduct includes, but is not limited to, the
10 following acts and/or omissions:

- 11 a. Failing to maintain an adequate data security system to reduce the risk of data
12 breaches and cyber-attacks;
- 13 b. Failing to adequately protect Private Information of current and former customers;
- 14 c. Failing to adequately protect current and former customers' Private Information;
- 15 d. Failing to properly monitor its own data security systems for existing intrusions,
16 brute-force attempts, and clearing of event logs;
- 17 e. Failing to apply all available security updates;
- 18 f. Failing to install the latest software patches, update its firewalls, check user account
19 privileges, or ensure proper security practices;
- 20 g. Failing to practice the principle of least-privilege and maintain credential hygiene;
- 21 h. Failing to avoid the use of domain-wide, administrator-level service accounts;
- 22 i. Failing to employ or enforce the use of strong randomized, just-in- time local
23 administrator passwords; and
- 24 j. Failing to properly train and supervise employees in the proper handling of inbound
25 emails.

26 50. As the result of computer systems in need of security upgrading and inadequate
27 procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to
28 safeguard Plaintiff and Class Members' Private Information.

***Data Breaches Put Victims at a Present Increased Risk of
Fraud and Identity Theft***

1 51. Defendant understood the Private Information it collected is highly sensitive, and of
2 significant value to those who would use it for wrongful purposes, such as the cyber-criminals who
3 perpetrated this Cyber-Attack.

4 52. The United States Government Accountability Office released a report in 2007
5 regarding data breaches (the “GAO Report”) in which it noted that victims of identity theft will
6 face “substantial costs and time to repair the damage to their good name and credit record.”⁵

7 53. The FTC recommends that identity theft victims take several steps to protect their
8 personal and financial information after a data breach, including contacting one of the credit
9 bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone
10 steals their identity), reviewing their credit reports, contacting companies to remove fraudulent
11 charges from their accounts, placing a credit freeze on their credit, and correcting their credit
12 reports.⁶ Identity thieves use stolen personal information such as Social Security numbers for a
variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

13 54. Identity thieves can also use Social Security numbers to obtain a driver license or
14 official identification card in the victim’s name but with the thief’s picture; use the victim’s name
15 and Social Security number to obtain government benefits; or file a fraudulent tax return using the
16 victim’s information.

17 55. In addition, identity thieves may obtain a job using the victim’s Social Security
18 number, rent a house or receive medical services in the victim’s name, and may even give the
19 victim’s personal information to police during an arrest resulting in an arrest warrant being issued
20 in the victim’s name.

21 56. A study by Identity Theft Resource Center shows the multitude of harms caused by
22 fraudulent use of personal and financial information.⁷

23 57. The value of personal data is axiomatic, considering the value of Big Data in
24 corporate America and the consequences of cyber thefts include heavy prison sentences. Even this
25

26 ⁵ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p.
27 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Apr. 12, 2019) (the
“GAO Report”).

28 ⁶ See <https://www.identitytheft.gov/Steps> (last visited Dec. 8, 2020).

⁷ See Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last accessed Dec. 10, 2020).

1 obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable
2 market value.

3 58. It must also be noted there may be a substantial time lag—measured in years—
4 between when harm occurs versus when it is discovered, and also between when Private
5 Information and/or financial information is stolen and when it is used. According to the U.S.
6 Government Accountability Office, which conducted a study regarding data breaches:

7 59. [L]aw enforcement officials told us that in some cases, stolen data may be held for
8 up to a year or more before being used to commit identity theft. Further, once stolen data have been
9 sold or posted on the Web, fraudulent use of that information may continue for years. As a result,
10 studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out
11 all future harm. *See* GAO Report at 29.

12 60. Private Information and financial information are such valuable commodities to
13 identity thieves that once the information has been compromised, criminals often trade the
14 information on the “cyber black-market” for years.

15 61. Indeed, a robust “cyber black market” exists in which criminals openly post stolen
16 Private Information on multiple underground Internet websites. Where the most private
17 information belonging to Plaintiff and Class Members was accessed and removed from
18 Defendant’s network, and entire batches of that stolen information already had been dumped by the
19 cyberthieves on the cyber black market, there is a strong probability that additional batches of
20 stolen information are yet to be dumped on the black market, meaning Plaintiff and Class Members
21 are at an increased risk of fraud and identity theft for many years into the future.

22 62. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts
23 for many years to come.

24 63. Sensitive information can sell for as much as \$363 according to the Infosec Institute.
25 PII is particularly valuable because criminals can use it to target victims with frauds and scams.
26 Once PII is stolen, fraudulent use of that information and damage to victims may continue for
27 years.

28 64. The PII of consumers remains of high value to criminals, as evidenced by the prices
they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
credentials. For example, personal information can be sold at a price ranging from \$40 to \$200.

1 65. Social Security numbers are among the worst kind of personal information to have
2 stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to
3 change. The Social Security Administration stresses that the loss of an individual's Social Security
4 number, as is the case here, can lead to identity theft and extensive financial fraud.

5 66. For example, the Social Security Administration has warned that identity thieves
6 can use an individual's Social Security number to apply for additional credit lines. Such fraud may
7 go undetected until debt collection calls commence months, or even years, later. Stolen Social
8 Security numbers also make it possible for thieves to file fraudulent tax returns, file for
9 unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities
10 is difficult to detect. An individual may not know that his or her Social Security number was used
11 to file for unemployment benefits until law enforcement notifies the individual's employer of the
12 suspected fraud. Fraudulent tax returns are typically discovered only when an individual's
13 authentic tax return is rejected.

14 67. Moreover, it is not an easy task to change or cancel a stolen Social Security number.
15 An individual cannot obtain a new Social Security number without significant paperwork and
16 evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he
17 credit bureaus and banks are able to link the new number very quickly to the old number, so all of
18 that old bad information is quickly inherited into the new Social Security number."⁸

19 68. This data, as one would expect, demands a much higher price on the black market.
20 Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card
21 information, personally identifiable information and Social Security numbers are worth more than
22 10x on the black market."⁹

23 69. At all relevant times, Defendant knew or reasonably should have known these risks,
24 the importance of safeguarding Private Information, and the foreseeable consequences if its data
25 security systems were breached and strengthened their data systems accordingly. Defendant was

26 ⁸ Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Feb. 9, 2015,
<http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last
27 visited Oct. 28, 2020).

28 ⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Feb. 6, 2015,
<http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>
(last visited Oct. 28, 2020).

1 put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to
2 properly prepare for that risk.

3 70. *Plaintiffs' and Class Members' Damages*

4 71. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' PII
5 secure are long lasting and severe. Once that kind of information is stolen, fraudulent use of that
6 information and damage to victims may continue for years. Consumer victims of data breaches are
7 more likely to become victims of identity fraud.¹⁰

8 72. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and
9 left inadequately protected by Defendant—who did not obtain Plaintiffs' or Class Members'
10 consent to disclose such information to any other person as required by applicable law and industry
11 standards.

12 73. The Data Breach was a direct and proximate result of Defendant's failure to: (a)
13 properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use,
14 and disclosure, as required by various state and federal regulations, industry practices, and common
15 law; (b) establish and implement appropriate administrative, technical, and physical safeguards to
16 ensure the security and confidentiality of Plaintiffs' and Class Members' PII; and (c) protect
17 against reasonably foreseeable threats to the security or integrity of such information.

18 74. Defendant had the resources necessary to prevent the Data Breach, but neglected to
19 adequately implement data security measures, despite its obligation to protect member data.

20 75. Defendant could have prevented the intrusions into its systems and, ultimately, the
21 theft of PII if Defendant had remedied the deficiencies in its data security systems and adopted
22 security measures recommended by experts in the field.

23 76. As a direct and proximate result of Defendant's wrongful actions and inactions,
24 Plaintiff and Class Members are now in imminent, immediate, and continuing increased risk of
25 harm from identity theft and fraud, requiring them to dedicate time and resources which they
26 otherwise would have dedicated to other life demands, such as work and family, to mitigate the
27 actual and potential impact of the Data Breach on their lives.

28 ¹⁰ 2014 Lexis.Nexis True Cost of Fraud Study, available at: <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last accessed Sept. 9, 2021)

1 77. The U.S. Department of Justice's Bureau of Justice Statistics found that "among
2 victims who had PII or PHI used for fraudulent purposes, 29% spent a month or more resolving
3 problems," and that "resolving the problems caused by identity theft [could] take more than a year
4 for some victims."¹¹

5 78. In the breach notification letter, Defendant did not much as even make an offer of
6 complementary identity monitoring services to its employees. Victims of data breaches and other
7 unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and
8 financial fraud, and Defendants fail to provide sufficient compensation for the unauthorized release
9 and disclosure of Plaintiffs' and Class Members' PII.

10 79. As a direct result of Defendant's failures to prevent the Data Breach, Plaintiff and
11 Class Members have suffered, will suffer, and are at increased risk of suffering:

- 12 a. The compromise, publication, theft and/or unauthorized use of their PII;
- 13 b. Out-of-pocket costs associated with the prevention, detection, recovery, and
14 remediation from identity theft or fraud;
- 15 c. Lost opportunity costs and lost wages associated with efforts expended and loss of
16 productivity from addressing and attempting to mitigate actual and future
17 consequences of the Data Breach, including but not limited to researching how to
18 prevent, detect, contest, and recover from identity theft and fraud;
- 19 d. The present and continued risk to their PII, which remains in the possession of
20 Defendant and is subject to further breaches so long as Defendant fails to undertake
21 appropriate measures to protect the PII in its possession; and
- 22 e. Current and future costs in terms of time, effort, and money that will be expended to
23 prevent, detect, contest, remediate, and repair the impact of the Data Breach for the
24 remainder of the lives of Plaintiff and Class Members.

25 80. In addition to a remedy for the economic harm, Plaintiff and Class Members
26 maintain an undeniable interest in ensuring their PII is secure, remains secure, and is not subject to
27 further misappropriation and theft.

28 ¹¹ U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft*, 2012, December 2013, available at: <https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last accessed Sept. 9, 2021).

1 81. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and
2 Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an
3 increased risk of future harm.

4 **CLASS ACTION ALLEGATIONS**

5 82. Plaintiff brings this suit on behalf of themselves and a class of similarly situated
6 individuals that are preliminarily defined as:

7
8 All individuals whose PII was compromised in the data breach announced by Samsung on
9 September 2, 2022, who reside in the State of California.

10 83. Excluded from the Class are the following individuals and/or entities: Defendant
11 and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former
12 employees, and any entity in which Defendant has a controlling interest; all individuals who make
13 a timely election to be excluded from this proceeding using the correct protocol for opting out; any
14 and all federal, state or local governments, including but not limited to their departments, agencies,
15 divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; Class counsel; and all
16 judges assigned to hear any aspect of this litigation, as well as their staff and immediate family
17 members.

18 84. Plaintiff reserves the right to modify or amend the definition of the proposed Class
19 before the Court determines whether certification is appropriate.

20 85. **Numerosity**: The Class is so numerous that joinder of all members is impracticable.
21 Defendant has identified more than 100 persons whose PII may have been improperly accessed in
22 the Data Breach, and the Class is identifiable within Defendant's records. A precise number of
23 class members can be ascertained through appropriate discovery and from records maintained by
24 Defendant.

25 86. **Commonality and Predominance**: Questions of law and fact common to the Class
26 exist and predominate over any questions affecting only individual Class members. These include
27 but are not limited to, the following:

- 28 a. Whether Plaintiffs' and the Class members' PII was accessed and/or viewed by one
or more unauthorized persons in the Data Breach alleged above;

- b. Whether Defendant's publishing Plaintiffs' and Class members' PII to unauthorized persons was permissible without the prior written authorization of the Plaintiff or the Class members;
- c. When and how Defendant should have learned and actually learned of the Data Breach;
- d. Whether Defendant's response to the Data Breach was adequate;
- e. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;
- f. Whether Defendant breached that duty;
- g. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class members' PII;
- h. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class members' PII;
- i. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII secure and prevent loss or misuse of that PII;
- j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- k. Whether Defendant caused Plaintiff and Class members damages;
- l. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their PII was compromised;
- m. Whether Plaintiff and Class members are entitled to actual damages, nominal and/or statutory damages, credit monitoring, other monetary relief, and/or equitable relief; and
- n. Whether Defendant violated the California Unfair Competition Law (Business & Professions Code § 17200 *et seq.*).

87. There are no defenses of a unique nature that may be asserted against the Plaintiff individually, as distinguished from the other Class Members, and the relief sought is common to the Class.

1 88. **Typicality**: Plaintiffs' claims are typical of those of other Class Members because
2 all had their PII compromised because of the Data Breach, due to Defendant's identical conduct.

3 89. **Adequacy of Representation**: Plaintiff will fairly and adequately represent and
4 protect the interests of the Class Members in that Plaintiffs' interests are aligned with the class.
5 Plaintiff have no disabling conflicts of interest that would be antagonistic to those of the other
6 members of the Class. Plaintiff seeks no relief that is adverse to Class Members. In addition,
7 Plaintiff retained counsel experienced in data breach and complex consumer class action litigation.
8 Neither Plaintiff nor their counsel have any interests which might cause them not to vigorously
9 pursue this claim.

10 90. **Superiority**: Class action treatment is superior to all other available methods for the
11 fair and efficient adjudication of the controversy alleged herein; it will permit a large number of
12 class members to prosecute their common claims in a single forum simultaneously, efficiently, and
13 without the unnecessary duplication of evidence, effort, and expense that hundreds of individual
14 actions would require. Class action treatment will permit the adjudication of relatively modest
15 claims by certain class members, who could not individually afford to litigate a complex claim
16 against large entities, such as Defendant. Further, even for those Class Members who could afford
17 to litigate such a claim, it would still be economically impractical and impose a burden on the
18 courts.

19 91. The prosecution of separate actions by individual members of the Class would
20 create a risk of inconsistent or varying adjudications with respect to individual members of the
21 Class, and a risk that any adjudications with respect to individual members of the Class would, as a
22 practical matter, either be dispositive of the interests of other members of the Class not party to the
23 adjudication or substantially impair or impede their ability to protect their interests.

24 92. Class certification is also warranted for purposes of injunctive and declaratory relief
25 because Defendant has acted, or refused to act, on grounds generally applicable to the class, so that
26 final injunctive and declaratory relief are appropriate with respect to the Class as a whole.

27 //

28 //

 //

 //

CLAIMS FOR RELIEF

First Claim for Relief

Negligence

(On Behalf of Plaintiff and the Class)

93. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set forth herein.

94. Defendant's own negligent conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's negligence included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's negligence also included its decision not to comply with

(1) industry standards, and/or best practices for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members; or (2) Section 5 of the FTC Act.

95. First, Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing its security protocols to ensure PII in Defendant's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on relevant cybersecurity measures. Defendant also had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiffs' and Class Members' PII.

96. As a condition of employment, Plaintiff and Class Members were obligated to provide Defendant with their PII. As such, Plaintiff and the Class Members entrusted their PII to Defendant with the understanding Defendant would safeguard their information.

97. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach. However, Plaintiff and Class Members had no ability to protect their PII in Defendant's possession.

98. Defendant had full knowledge of the sensitivity of the PII, and the types of harm Plaintiff and Class Members could, would, and will suffer if the information were wrongfully disclosed.

1 99. Defendant admitted that its computer system containing Plaintiffs' and Class
2 Members' PII was wrongfully compromised and accessed by unauthorized third persons, and that
3 the Data Breach occurred due to Defendant's actions and/or omissions.

4 100. Plaintiff and Class Members were the foreseeable and probable victims of
5 Defendant's negligent and inadequate security practices and procedures that led to the Data Breach.
6 Defendant knew or should have known of the inherent risks in collecting and storing the highly
7 valuable PII of Plaintiff and Class Members, the critical importance of providing adequate security
8 of that information, the current cyber security risks being perpetrated, and that Defendant had
9 inadequate employee training, monitoring and education and IT security protocols in place to
10 secure the PII of Plaintiff and Class Members.

11 101. Defendant negligently, through its actions and/or omissions, and unlawfully
12 breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in
13 protecting and safeguarding Plaintiffs' and Class Members' PII while the information was within
14 Defendant's possession and/or control by failing to comply with and/or deviating from standard
15 industry rules, regulations, and practices at the time of the Data Breach.

16 102. Second, Defendant's violations of Section 5 of the FTC Act constitute negligence.
17 Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as
18 interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of
19 failing to use reasonable measures to protect PII. The FTC publications and orders described above
20 also form part of the basis of Defendant's duty in this regard.

21 103. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures
22 to protect Plaintiffs' and Class members' PII and not complying with applicable industry standards,
23 as described in detail herein. Defendant's conduct was particularly unreasonable given the nature
24 and amount of PII it required, obtained, and stored, and the foreseeable consequences of a data
25 breach including, specifically, the damages that would result to Plaintiff and Class members.

26 104. Plaintiff and Class Members are within the class of persons the FTC Act was
27 intended to protect.

28 105. The harm the Data Breach caused, and continues to cause, is the type of harm the
FTC Act was intended to guard against. The FTC pursues enforcement actions against businesses,

1 which, as a result of their failure to employ reasonable data security measures and avoid unfair and
2 deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

3 106. Defendant, through its actions and/or omissions, unlawfully breached its duty to
4 Plaintiff and Class Members by failing to have appropriate procedures in place to detect and
5 prevent unauthorized dissemination of Plaintiffs' and Class Members' PII.

6 107. Defendant, through its actions and/or omissions, unlawfully breached its duty to
7 adequately disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

8 108. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and
9 Class Members, Plaintiffs' and Class Members' PII would not have been compromised.

10 109. There is a temporal and close causal connection between Defendant's failure to
11 implement security measures to protect the PII and the harm suffered, and/or risk of present and
12 continual harm suffered, by Plaintiff and Class Members.

13 110. As a direct and proximate result of Defendant's negligence, Plaintiff and Class
14 Members have suffered, and continue to suffer, injuries and damages arising from the Data Breach,
15 including, but not limited to: damages from lost time and efforts to mitigate the actual and potential
16 impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts"
17 with credit reporting agencies, contacting their financial institutions, closely reviewing and
18 monitoring their credit reports and various accounts for unauthorized activity, filing police reports,
19 and damages from identity theft, which may take months—if not years—to discover, detect, and
20 remedy.

21 111. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff
22 and Class Members have suffered, and will continue to suffer, the continued risks of exposure of
23 their PII, which remains in Defendant's possession and is subject to further unauthorized
24 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
25 the PII in its continued possession.

26 **Second Claim for Relief**

27 **Negligence *Per Se***

28 **(On Behalf of Plaintiff and the Class)**

112. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set
forth herein.

1 113. Pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45, Defendant had a duty to
2 provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and
3 Class Members' Private Information.

4 114. Plaintiff and Class Members are within the class of persons that the FTC Act was
5 intended to protect.

6 115. The harm that occurred as a result of the Data Breach is the type of harm the FTC
7 Act was intended to guard against. The FTC has pursued enforcement actions against businesses,
8 which, as a result of their failure to employ reasonable data security measures and avoid unfair and
9 deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

10 116. Defendant breached its duties to Plaintiff and Class Members under the Federal
11 Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and
12 data security practices to safeguard Plaintiffs' and Class Members' Private Information.

13 117. Defendant's failure to comply with applicable laws and regulations constitutes
14 negligence *per se*.

15 118. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff
16 and Class Members, Plaintiff and Class Members would not have been injured.

17 119. The injury and harm suffered by Plaintiff and Class Members was the reasonably
18 foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it
19 was failing to meet their duties, and that Defendant's breach would cause Plaintiff and Class
20 Members to experience the foreseeable harms associated with the exposure of their Private
21 Information.

22 120. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and
23 Class Members have suffered injury and are entitled to compensatory, consequential, and punitive
24 damages in an amount to be proven at trial.

25 **Third Claim for Relief**

26 **Breach of Implied Contract**

27 **(On Behalf of Plaintiff and the Class)**

28 121. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set
forth herein.

1 122. Plaintiff and Class Members were required to provide their PII to Defendant as a
2 condition of purchase.

3 123. Plaintiff and Class Members provided their PII to Defendant in exchange for
4 products/services, along with Defendant's promise to protect their PII from unauthorized
5 disclosure.

6 124. Upon information and belief, in its written privacy policies, Defendant expressly
7 promised Plaintiff and Class Members that it would only disclose PII under certain circumstances,
8 none of which relate to the Data Breach.

9 125. 135. Implicit in the agreement between Plaintiff and Class Members on the one
10 hand, and Defendant on the other, regarding providing PII, was Defendant's obligation to: (a) use
11 such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent
12 unauthorized disclosures of the PII; (d) provide Plaintiff and Class Members with prompt and
13 sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably
14 safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses;
15 and (f) retain the PII only under conditions that kept such information secure and confidential.

16 126. Without such implied contracts, Plaintiff and Class Members would not have
17 provided their PII to Defendant.

18 127. Plaintiff and Class Members fully performed their obligations under the implied
19 contract with Defendant. However, Defendant did not.

20 128. Defendant breached the implied contracts with Plaintiff and Class members by
21 failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII, which was
22 compromised as a result of the Data Breach.

23 129. As a direct and proximate result of Defendant's breach of the implied contracts,
24 Plaintiff and Class Members have suffered, and continue to suffer, injuries and damages arising
25 from the Data Breach including, but not limited to: damages from lost time and effort to mitigate
26 the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing
27 "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing
28 or modifying financial accounts, closely reviewing and monitoring their credit reports and various
accounts for unauthorized activity, filing police reports, and damages from identity theft, which
may take months if not years to discover, detect, and remedy.

Fourth Claim for Relief

Breach of Confidence

(On Behalf of Plaintiff and the Class)

130. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set forth herein.

131. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiff and Class Members provided to Defendant.

132. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

133. Plaintiff and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the information to be disseminated to any unauthorized parties.

134. Plaintiff and Class Members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of protecting its networks and data systems.

135. Defendant required and voluntarily received, in confidence, Plaintiffs' and Class Members' PII with the understanding that the information would not be disclosed or disseminated to the public or any unauthorized third parties.

136. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

137. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered, and will continue to suffer damages.

1 138. But for Defendant's disclosure of Plaintiffs' and Class Members' PII in violation of
2 the parties' understanding of confidence, Plaintiffs' and Class Members' PII would not have been
3 compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data
4 Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as
5 the resulting damages.

6 139. The injury and harm Plaintiff and Class Members suffered, and continue to suffer,
7 was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and
8 Class Members' PII. Defendant knew its computer systems and technologies for accepting and
9 securing Plaintiffs' and Class Members' PII had numerous security and other vulnerabilities
10 placing Plaintiffs' and Class Members' PII in jeopardy.

11 140. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff
12 and Class Members have suffered and will suffer injury, including but not limited to: (a) actual
13 identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses
14 associated with the prevention, detection, and recovery from identity theft and/or unauthorized use
15 of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity
16 addressing and attempting to mitigate the actual and future consequences of the Data Breach,
17 including but not limited to efforts spent researching how to prevent, detect, contest, and recover
18 from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and
19 is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate
20 and adequate measures to protect the PII in its continued possession; (f) future costs in terms of
21 time, effort, and money that will be expended as result of the Data Breach for the remainder of the
22 lives of Plaintiff and Class Members; and (g) the diminished value of Defendant's services they
23 received.

24 141. As a direct and proximate result of Defendant's breaches of its fiduciary duties,
25 Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or
26 harm, and other economic and non-economic losses.

27 //

28 //

 //

 //

Fifth Claim for Relief

**Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200 *et seq.*--Unfair Business Practices
(On Behalf of Plaintiff and the Class)**

142. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set forth herein.

143. Defendant violated California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* (“UCL”), by engaging in unlawful, unfair, or fraudulent business acts and practices, and unfair, deceptive, untrue, or misleading advertising that constitute acts of “unfair competition” as defined in Cal. Bus. & Prof. Code § 17200 with respect to the services provided to Plaintiff and California Subclass Members.

144. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff and California Subclass Members’ PII with knowledge the information would not be adequately protected; and by storing Plaintiffs’ and California Subclass Members’ PII in an unsecure electronic environment in violation of California’s data breach statute, Cal. Civ. Code § 1798.81.5, which require Defendant to take reasonable methods of safeguarding the PII of Plaintiff and California Subclass Members.

145. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

146. As a direct and proximate result of Defendant’s unlawful practices and acts, Plaintiff and California Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiff and California Subclass Members’ legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

147. Defendant knew or should have known Defendant’s computer systems and data security practices were inadequate to safeguard Plaintiff and California Subclass Members’ PII and that the risk of a data breach or theft was highly likely. Defendant’s actions in engaging in the

1 above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and
2 reckless with respect to the rights of Plaintiff and the California Subclass Members.

3 148. Plaintiff, on behalf of the California Subclass, seeks relief under the UCL,
4 including, but not limited to, restitution to Plaintiff and California Subclass Members of money or
5 property Defendant may have acquired by means of Defendant's unlawful, and unfair business
6 practices, restitutionary disgorgement of all monies that accrued to Defendant because of
7 Defendant's unlawful and unfair business practices, declaratory relief, attorney fees and costs
8 (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

9 **Sixth Claim for Relief**

10 **Violation of the California Consumer Privacy Act,**

11 **Cal. Civ. Code § 1798.150 *et seq.***

12 **(On Behalf of Plaintiff and the Class)**

13 149. Plaintiff re-allege and incorporate by reference the Paragraphs above as if fully set
14 forth herein.

15 150. Defendant is a corporation organized or operated for the profit or financial benefit
16 of its owners with annual gross revenues over \$200 billion.

17 151. Defendant collects consumers' personal information as defined in Cal. Civ. Code §
18 1798.140.

19 152. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and
20 Class members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as
21 a result of Defendant's violations of its duty to implement and maintain reasonable security
22 procedures and practices appropriate to the nature of the information.

23 153. Defendant collects consumers' personal information as defined in Cal. Civ. Code §
24 1798.140. Defendant has a duty to implement and maintain reasonable security procedures and
25 practices to protect this personal information. As identified herein, Defendant failed to do so.

26 154. As a direct and proximate result of Defendant's acts, Plaintiff's and Class members'
27 personal information was subjected to unauthorized access and exfiltration, theft, or disclosure.

28 155. Plaintiff and Class members seek injunctive or other equitable relief to ensure
Defendant hereinafter adequately safeguard customers' PII by implementing reasonable security
procedures and practices. Such relief is particularly important because Defendant continues to hold

1 customers' PII, including Plaintiff's and Class members' PII. These individuals have an interest in
2 ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing
3 to adequately safeguard this information, as evidenced by its multiple data breaches.

4 156. On September 16, 2022, Plaintiff's counsel sent a notice letter to Samsung's
5 corporate headquarters in New Jersey via USPS certified mail. Since Samsung cannot cure the
6 Data Breach within 30 days, and Plaintiff believes such cure is not possible under these facts and
7 circumstances, then Plaintiff intends to seek actual damages and statutory damages of \$750 per
8 customer record subject to the Data Breach on behalf of the Class as permitted by the CCPA.

9
10 **PRAYER FOR RELIEF**

11 **WHEREFORE**, Plaintiffs, on behalf of themselves and all Class Members, request that the
12 Court grant judgment against Defendant as follows:

- 13 a. An order certifying the Class as defined herein, and appointing Plaintiff and their
14 Counsel to represent the Class;
- 15 b. Injunctive relief requested by Plaintiffs, including but not limited to, injunctive and
16 other equitable relief as is necessary to protect the interests of Plaintiff and Class
17 Members, including but not limited to an order:
- 18 i. prohibiting Defendant from engaging in the wrongful and unlawful acts
19 described herein,
- 20 ii. requiring Defendant to protect, including through encryption, all data
21 collected through the course of its business in accordance with all applicable
22 regulations, industry standards, and federal, state or local laws,
- 23 iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff and
24 Class members unless Defendant can provide to the Court reasonable
25 justification for the retention and use of such information when weighed
26 against the privacy interests of Plaintiff and Class Members,
- 27 iv. requiring Defendant to implement and maintain a comprehensive
28 Information Security Program designed to protect the confidentiality and
integrity of the PII of Plaintiff and Class Members,

- v. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII on a cloud-based database,
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring,
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures,
- ix. requiring Defendant to conduct regular database scanning and securing checks,
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members,
- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,
- xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII,
- xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

- 1 Defendant's information networks for threats, both internal and external, and
2 assess whether monitoring tools are appropriately configured, tested, and
3 updated,
- 4 xiv. requiring Defendant to meaningfully educate all Class Members about the
5 threats that they face as a result of the loss of their PII to third parties, as
6 well as the steps affected individuals must take to protect themselves,
- 7 xv. requiring Defendant to design, maintain, and test its computer systems to
8 ensure that PII in its possession is adequately secured and protected,
- 9 xvi. requiring Defendant disclose any future data disclosures in a timely and
10 accurate manner; and
- 11 xvii. requiring Defendant to provide ongoing credit monitoring and identity theft
12 repair services to Class Members.
- 13 c. An award of compensatory, statutory, and nominal damages in an amount to be
14 determined, including statutory damages under the CCPA;
- 15 d. An award for equitable relief requiring restitution and disgorgement of the revenues
16 wrongfully retained as a result of Defendant's wrongful conduct;
- 17 e. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable
18 by law; and
- 19 f. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

20 Plaintiff hereby demands a trial by jury.

21 **SROURIAN LAW FIRM, PC**

22 

23
24 DATED: October 18, 2022

25 By: _____
26 Daniel Srourian, Esq.
27 Attorney for Plaintiff and the
28 [Proposed] Class

PROOF OF SERVICE
(§ 1013a, 2015.5 C.C.P.)

STATE OF CALIFORNIA)
) ss.
COUNTY OF LOS ANGELES)

I am a citizen of the United States of America; I am over the age of eighteen years and not a party to the within entitled action; my business address is: 3435 Wilshire Boulevard, Suite 1710, Los Angeles, California 90010.

On the below-indicated date, I served the following document:

**PLAINTIFF'S REPLY IN SUPPORT OF MOTION FOR AN ORDER TO COMPEL
DEFENDANT TO PROVIDE FURTHER RESPONSES TO:**

on the interested parties in said action by placing

___X___ a true and correct copy,

and addressed as set forth on the attached Service List and delivered by one or more of the means set forth below:

☒ **BY MAIL:** I deposited such envelope in the mail at Los Angeles, California. The envelope was mailed with postage thereon fully prepaid. As follows: I am "readily familiar" with the firm's practice of collection and processing correspondence for mailing. Under that practice it would be deposited with U.S. postal service on that same day with postage thereon fully prepaid at Los Angeles, California in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

EXECUTED: 10/18/22
At Los Angeles, California



DANIEL SROURIAN

SERVICE LIST

Counsel	Party
SAMSUNG ELECTRONICS AMERICA, INC. 85 CHALLENGER ROAD RIDGEFIELD PARK, NJ 07660 C T CORPORATION SYSTEM C/O SAMSUNG ELECTRONICS AMERICA, INC. 330 N BRAND BLVD STE 700 GLENDALE, CA 91203	<i>Defendants</i>

NAME, ADDRESS, AND TELEPHONE NUMBER OF ATTORNEY OR PARTY WITHOUT ATTORNEY: Daniel Srourian, Esq. Srourian Law Firm, P.C. 3435 Wilshire Blvd. Suite 1710 Los Angeles, CA 90010	STATE BAR NUMBER: 285678	Reserved for Clerk's File Stamp
ATTORNEY FOR (Name): Raffi Kelechian		
SUPERIOR COURT OF CALIFORNIA, COUNTY OF LOS ANGELES		
COURTHOUSE ADDRESS: 111 N. Hill St. Los Angeles, CA 90012		
PLAINTIFF/PETITIONER: Raffi Kelechian		
DEFENDANT/RESPONDENT: SAmsung International		CASE NUMBER: 22STCV30284
PEREMPTORY CHALLENGE TO JUDICIAL OFFICER (Code Civ. Proc., § 170.6)		

Name of Judicial Officer: (PRINT) William F. Highberger	Dept. Number: 10
<input checked="" type="checkbox"/> Judge <input type="checkbox"/> Commissioner <input type="checkbox"/> Referee	

I am a party (or attorney for a party) to this action or special proceeding. The judicial officer named above, before whom the trial of, or a hearing in, this case is pending, or to whom it has been assigned, is prejudiced against the party (or his or her attorney) or the interest of the party (or his or her attorney), so that declarant cannot, or believes that he or she cannot, have a fair and impartial trial or hearing before the judicial officer.

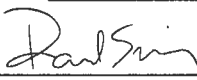
DECLARATION

I declare under penalty of perjury, under the laws of the State of California, that the information entered on this form is true and correct.

Filed on behalf of: Raffi Kelechian
Name of Party

☒ Plaintiff/Petitioner ☐ Cross Complainant
☐ Defendant/Respondent ☐ Cross Defendant
☐ Other: _____

Dated: 09/28/22


Signature of Declarant

Daniel Srourian

Printed Name

Print

Save

Clear

SUPERIOR COURT OF CALIFORNIA, COUNTY OF LOS ANGELES Branch Name: Spring Street Courthouse Mailing Address: 312 North Spring Street City, State and Zip Code: Los Angeles CA 90012	
SHORT TITLE: RAFFI KELECHIAN vs SAMSUNG ELECTRONICS AMERICA, INC. NOTICE OF CONFIRMATION OF ELECTRONIC FILING	CASE NUMBER: 22STCV30284

The Electronic Filing described by the below summary data was reviewed and accepted by the Superior Court of California, County of LOS ANGELES. In order to process the filing, the fee shown was assessed.

Electronic Filing Summary Data

Electronically Submitted By: DDS Legal Services
Reference Number: JTI291496
Submission Number: 22LA01162173
Court Received Date: 09/16/2022
Court Received Time: 12:29 pm
Case Number: 22STCV30284
Case Title: RAFFI KELECHIAN vs SAMSUNG ELECTRONICS AMERICA, INC.
Location: Spring Street Courthouse
Case Type: Civil Unlimited
Case Category: Other Commercial/Business Tort (not fraud/ breach of contract)
Jurisdictional Amount: Over \$25,000
Notice Generated Date: 09/16/2022
Notice Generated Time: 1:00 pm

Documents Electronically Filed/Received

Status

Complaint

Accepted

Civil Case Cover Sheet

Rejected

Reject Reason(s):
Other: Address is incorrect

Summons

Accepted

Comments

Submitter's Comments:

Clerk's Comments:

Electronic Filing Service Provider Information

Service Provider: DDS Legal Services

Contact: DDS Legal Services

Phone: (714) 662-5555

SUPERIOR COURT OF CALIFORNIA COUNTY OF LOS ANGELES	<small>Reserved for Clerk's File Stamp</small> FILED Superior Court of California County of Los Angeles 09/16/2022 By <u>R. Lozano</u> Deputy Clerk
COURTHOUSE ADDRESS: Spring Street Courthouse 312 North Spring Street, Los Angeles, CA 90012	
NOTICE OF CASE ASSIGNMENT UNLIMITED CIVIL CASE	
Your case is assigned for all purposes to the judicial officer indicated below.	CASE NUMBER 22STCV30284

THIS FORM IS TO BE SERVED WITH THE SUMMONS AND COMPLAINT

	ASSIGNED JUDGE	DEPT	ROOM		ASSIGNED JUDGE	DEPT	ROOM
✓	William F. Highberger	10					

Given to the Plaintiff/Cross-Complainant/Attorney of Record Sherri R. Carter, Executive Officer / Clerk of Court
 on 09/16/2022 (Date) By R. Lozano, Deputy Clerk

INSTRUCTIONS FOR HANDLING UNLIMITED CIVIL CASES

The following critical provisions of the California Rules of Court, Title 3, Division 7, as applicable in the Superior Court, are summarized for your assistance.

APPLICATION

The Division 7 Rules were effective January 1, 2007. They apply to all general civil cases.

PRIORITY OVER OTHER RULES

The Division 7 Rules shall have priority over all other Local Rules to the extent the others are inconsistent.

CHALLENGE TO ASSIGNED JUDGE

A challenge under Code of Civil Procedure Section 170.6 must be made within **15** days after notice of assignment for all purposes to a judge, or if a party has not yet appeared, within 15 days of the first appearance.

TIME STANDARDS

Cases assigned to the Independent Calendaring Courts will be subject to processing under the following time standards:

COMPLAINTS

All complaints shall be served within 60 days of filing and proof of service shall be filed within 90 days.

CROSS-COMPLAINTS

Without leave of court first being obtained, no cross-complaint may be filed by any party after their answer is filed. Cross-complaints shall be served within 30 days of the filing date and a proof of service filed within 60 days of the filing date.

STATUS CONFERENCE

A status conference will be scheduled by the assigned Independent Calendar Judge no later than 270 days after the filing of the complaint. Counsel must be fully prepared to discuss the following issues: alternative dispute resolution, bifurcation, settlement, trial date, and expert witnesses.

FINAL STATUS CONFERENCE

The Court will require the parties to attend a final status conference not more than 10 days before the scheduled trial date. All parties shall have motions in limine, bifurcation motions, statements of major evidentiary issues, dispositive motions, requested form jury instructions, special jury instructions, and special jury verdicts timely filed and served prior to the conference. These matters may be heard and resolved at this conference. At least five days before this conference, counsel must also have exchanged lists of exhibits and witnesses, and have submitted to the court a brief statement of the case to be read to the jury panel as required by Chapter Three of the Los Angeles Superior Court Rules.

SANCTIONS

The court will impose appropriate sanctions for the failure or refusal to comply with Chapter Three Rules, orders made by the Court, and time standards or deadlines established by the Court or by the Chapter Three Rules. Such sanctions may be on a party, or if appropriate, on counsel for a party.

This is not a complete delineation of the Division 7 or Chapter Three Rules, and adherence only to the above provisions is therefore not a guarantee against the imposition of sanctions under Trial Court Delay Reduction. Careful reading and compliance with the actual Chapter Rules is imperative.

Class Actions

Pursuant to Local Rule 2.3, all class actions shall be filed at the Stanley Mosk Courthouse and are randomly assigned to a complex judge at the designated complex courthouse. If the case is found not to be a class action it will be returned to an Independent Calendar Courtroom for all purposes.

***Provisionally Complex Cases**

Cases filed as provisionally complex are initially assigned to the Supervising Judge of complex litigation for determination of complex status. If the case is deemed to be complex within the meaning of California Rules of Court 3.400 et seq., it will be randomly assigned to a complex judge at the designated complex courthouse. If the case is found not to be complex, it will be returned to an Independent Calendar Courtroom for all purposes.

FILED
Superior Court of California
County of Los Angeles

MAY 03 2019

Sherri R. Carter, Executive Officer/Clerk

By Rizalinda Mina, Deputy
Rizalinda Mina

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF LOS ANGELES

IN RE LOS ANGELES SUPERIOR COURT) FIRST AMENDED GENERAL ORDER
— MANDATORY ELECTRONIC FILING)
FOR CIVIL)
)
)
)

On December 3, 2018, the Los Angeles County Superior Court mandated electronic filing of all documents in Limited Civil cases by litigants represented by attorneys. On January 2, 2019, the Los Angeles County Superior Court mandated electronic filing of all documents filed in Non-Complex Unlimited Civil cases by litigants represented by attorneys. (California Rules of Court, rule 2.253(b).) All electronically filed documents in Limited and Non-Complex Unlimited cases are subject to the following:

1) DEFINITIONS

- a) **“Bookmark”** A bookmark is a PDF document navigational tool that allows the reader to quickly locate and navigate to a designated point of interest within a document.
- b) **“Efiling Portal”** The official court website includes a webpage, referred to as the efiling portal, that gives litigants access to the approved Electronic Filing Service Providers.
- c) **“Electronic Envelope”** A transaction through the electronic service provider for submission of documents to the Court for processing which may contain one or more PDF documents attached.
- d) **“Electronic Filing”** Electronic Filing (eFiling) is the electronic transmission to a Court of a document in electronic form. (California Rules of Court, rule 2.250(b)(7).)

- e) **“Electronic Filing Service Provider”** An Electronic Filing Service Provider (EFSP) is a person or entity that receives an electronic filing from a party for retransmission to the Court. In the submission of filings, the EFSP does so on behalf of the electronic filer and not as an agent of the Court. (California Rules of Court, rule 2.250(b)(8).)
- f) **“Electronic Signature”** For purposes of these local rules and in conformity with Code of Civil Procedure section 17, subdivision (b)(3), section 34, and section 1010.6, subdivision (b)(2), Government Code section 68150, subdivision (g), and California Rules of Court, rule 2.257, the term “Electronic Signature” is generally defined as an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record.
- g) **“Hyperlink”** An electronic link providing direct access from one distinctively marked place in a hypertext or hypermedia document to another in the same or different document.
- h) **“Portable Document Format”** A digital document format that preserves all fonts, formatting, colors and graphics of the original source document, regardless of the application platform used.

2) MANDATORY ELECTRONIC FILING

a) Trial Court Records

Pursuant to Government Code section 68150, trial court records may be created, maintained, and preserved in electronic format. Any document that the Court receives electronically must be clerically processed and must satisfy all legal filing requirements in order to be filed as an official court record (California Rules of Court, rules 2.100, et seq. and 2.253(b)(6)).

b) Represented Litigants

Pursuant to California Rules of Court, rule 2.253(b), represented litigants are required to electronically file documents with the Court through an approved EFSP.

c) Public Notice

The Court has issued a Public Notice with effective dates the Court required parties to electronically file documents through one or more approved EFSPs. Public Notices containing effective dates and the list of EFSPs are available on the Court’s website, at www.lacourt.org.

d) Documents in Related Cases

Documents in related cases must be electronically filed in the eFiling portal for that case type if electronic filing has been implemented in that case type, regardless of whether the case has been related to a Civil case.

3) EXEMPT LITIGANTS

a) Pursuant to California Rules of Court, rule 2.253(b)(2), self-represented litigants are exempt from mandatory electronic filing requirements.

b) Pursuant to Code of Civil Procedure section 1010.6, subdivision (d)(3) and California Rules of Court, rule 2.253(b)(4), any party may make application to the Court requesting to be excused from filing documents electronically and be permitted to file documents by conventional means if the party shows undue hardship or significant prejudice.

4) EXEMPT FILINGS

a) The following documents shall not be filed electronically:

i) Peremptory Challenges or Challenges for Cause of a Judicial Officer pursuant to Code of Civil Procedure sections 170.6 or 170.3;

ii) Bonds/Undertaking documents;

iii) Trial and Evidentiary Hearing Exhibits

iv) Any ex parte application that is filed concurrently with a new complaint including those that will be handled by a Writs and Receivers department in the Mosk courthouse; and

v) Documents submitted conditionally under seal. The actual motion or application shall be electronically filed. A courtesy copy of the electronically filed motion or application to submit documents conditionally under seal must be provided with the documents submitted conditionally under seal.

b) Lodgments

Documents attached to a Notice of Lodgment shall be lodged and/or served conventionally in paper form. The actual document entitled, "Notice of Lodgment," shall be filed electronically.

//

//

5) ELECTRONIC FILING SYSTEM WORKING PROCEDURES

Electronic filing service providers must obtain and manage registration information for persons and entities electronically filing with the court.

6) TECHNICAL REQUIREMENTS

a) Electronic documents must be electronically filed in PDF, text searchable format **when** technologically feasible without impairment of the document's image.

b) The table of contents for any filing must be bookmarked.

c) Electronic documents, including but not limited to, declarations, proofs of service, and exhibits, must be bookmarked within the document pursuant to California Rules of Court, rule 3.1110(f)(4). Electronic bookmarks must include links to the first page of each bookmarked item (e.g. exhibits, declarations, deposition excerpts) and with bookmark titles that identify the bookmarked item and briefly describe the item.

d) Attachments to primary documents must be bookmarked. Examples include, but are not limited to, the following:

i) Depositions;

ii) Declarations;

iii) Exhibits (including exhibits to declarations);

iv) Transcripts (including excerpts within transcripts);

v) Points and Authorities;

vi) Citations; and

vii) Supporting Briefs.

e) Use of hyperlinks within documents (including attachments and exhibits) is strongly encouraged.

f) Accompanying Documents

Each document accompanying a single pleading must be electronically filed as a **separate** digital PDF document.

g) Multiple Documents

Multiple documents relating to one case can be uploaded in one envelope transaction.

h) Writs and Abstracts

Writs and Abstracts must be submitted as a separate electronic envelope.

i) Sealed Documents

If and when a judicial officer orders documents to be filed under seal, those documents must be filed electronically (unless exempted under paragraph 4); the burden of accurately designating the documents as sealed at the time of electronic submission is the submitting party's responsibility.

j) Redaction

Pursuant to California Rules of Court, rule 1.201, it is the submitting party's responsibility to redact confidential information (such as using initials for names of minors, using the last four digits of a social security number, and using the year for date of birth) so that the information shall not be publicly displayed.

7) ELECTRONIC FILING SCHEDULE

a) Filed Date

i) Any document received electronically by the court between 12:00 am and 11:59:59 pm shall be deemed to have been effectively filed on that court day if accepted for filing. Any document received electronically on a non-court day, is deemed to have been effectively filed on the next court day if accepted. (California Rules of Court, rule 2.253(b)(6); Code Civ. Proc. § 1010.6(b)(3).)

ii) Notwithstanding any other provision of this order, if a digital document is not filed in due course because of: (1) an interruption in service; (2) a transmission error that is not the fault of the transmitter; or (3) a processing failure that occurs after receipt, the Court may order, either on its own motion or by noticed motion submitted with a declaration for Court consideration, that the document be deemed filed and/or that the document's filing date conform to the attempted transmission date.

8) EX PARTE APPLICATIONS

a) Ex parte applications and all documents in support thereof must be electronically filed no later than 10:00 a.m. the court day before the ex parte hearing.

- b) Any written opposition to an ex parte application must be electronically filed by 8:30 a.m. the day of the ex parte hearing. A printed courtesy copy of any opposition to an ex parte application must be provided to the court the day of the ex parte hearing.

9) PRINTED COURTESY COPIES

- a) For any filing electronically filed two or fewer days before the hearing, a courtesy copy must be delivered to the courtroom by 4:30 p.m. the same business day the document is efiled. If the efiled is submitted after 4:30 p.m., the courtesy copy must be delivered to the courtroom by 10:00 a.m. the next business day.
- b) Regardless of the time of electronic filing, a printed courtesy copy (along with proof of electronic submission) is required for the following documents:
- i) Any printed document required pursuant to a Standing or General Order;
 - ii) Pleadings and motions (including attachments such as declarations and exhibits) of 26 pages or more;
 - iii) Pleadings and motions that include points and authorities;
 - iv) Demurrers;
 - v) Anti-SLAPP filings, pursuant to Code of Civil Procedure section 425.16;
 - vi) Motions for Summary Judgment/Adjudication; and
 - vii) Motions to Compel Further Discovery.
- c) Nothing in this General Order precludes a Judicial Officer from requesting a courtesy copy of additional documents. Courtroom specific courtesy copy guidelines can be found at www.lacourt.org on the Civil webpage under "Courtroom Information."

10) WAIVER OF FEES AND COSTS FOR ELECTRONICALLY FILED DOCUMENTS

- a) Fees and costs associated with electronic filing must be waived for any litigant who has received a fee waiver. (California Rules of Court, rules 2.253(b)(), 2.258(b), Code Civ. Proc. § 1010.6(d)(2).)
- b) Fee waiver applications for waiver of court fees and costs pursuant to Code of Civil Procedure section 1010.6, subdivision (b)(6), and California Rules of Court, rule 2.252(f), may be electronically filed in any authorized action or proceeding.


1 11) SIGNATURES ON ELECTRONIC FILING

2 For purposes of this General Order, all electronic filings must be in compliance with California
3 Rules of Court, rule 2.257. This General Order applies to documents filed within the Civil
4 Division of the Los Angeles County Superior Court.

5
6 This First Amended General Order supersedes any previous order related to electronic filing,
7 and is effective immediately, and is to remain in effect until otherwise ordered by the Civil
8 Supervising Judge and/or Presiding Judge.

9
10 DATED: May 3, 2019




KEVIN C. BRAZILE
Presiding Judge